University of Colorado Colorado Springs

UCCS CAMPUS POLICY

Policy Title: HIPAA Compliance Policy

Policy Number: 100-020	**Policy Functional Area:** Administration/Organization
Effective:	January 17, 2023
Approved by:	Venkat Reddy, Chancellor
Responsible Vice Chancellor:	Chancellor
Office of Primary Responsibility:	UCCS Compliance
Policy Primary Contact:	UCCS Director of Campus Compliance, 719-255-3837
Supersedes:	February 20, 1995; April 19, 2004, January 14, 2013
Last Reviewed/Updated:	November 29, 2022
Applies to:	Administrators, Faculty, Staff, Students

Reason for Policy: This policy was established to comply with the Health Insurance Portability and Accountability Act (HIPAA) for UCCS *designated health care components*.

I. INTRODUCTION

The University of Colorado Colorado Springs ("UCCS" or "University") has adopted this HIPAA Compliance Policy to comply with the Health Insurance Portability and Accountability Act (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

II. POLICY STATEMENT

A. General. In general, HIPAA addresses *protected health information (PHI)* that is maintained or transmitted by a *covered entity (CE).* UCCS takes all actions required to comply with the HIPAA.

1. UCCS hereby acknowledges our duty and responsibility to protect the privacy and security of individually identifiable health information (IIHI) generally, and *PHI* as defined in the HIPAA Regulations, under the regulations implementing HIPAA, and other federal and state laws protecting the confidentiality of personal information. UCCS also acknowledges our duty and responsibility to support and facilitate the timely and unimpeded flow of *health information* for lawful and appropriate purposes.
2. UCCS shall develop and implement written privacy policies and procedures that are consistent with the HIPAA Rules and UCCS Policy 100-001 Campus Policy Process. If necessary, each UCCS *designated health care component* will develop department/unit level policies and procedures.

B. Scope. The University of Colorado has a *hybrid entity designation* as defined below in the key terms. This policy applies to UCCS *designated health care components* and their *workforce members* as defined below in the key terms. The *designated health care components* for UCCS can be found in the University's Administrative Policy Statement (APS) 5055 HIPAA Hybrid Entity Designation Exhibit A. All *workforce members* associated with UCCS *designated health care components* must read, understand, and comply with this policy in full and at all times.
C. Compliance and Enforcement. UCCS and its *designated health care components* must comply with HIPAA, the HIPAA implementing regulations, in accordance with the requirements at 45 CFR Parts 160 and 164, as amended, and this policy. Full compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties. All UCCS *designated health care component* directors and managers, as well as the *privacy officer* and *security officer*, are responsible for enforcing this policy.
D. Privacy and Security Personnel. UCCS will designate and maintain at all times an active *privacy officer* and *security officer*. The UCCS *privacy officer* and UCCS *security officer* are responsible for developing and implementing its campus-wide policies and procedures and training related to HIPAA. The *privacy officer* will serve as the contact person responsible for receiving complaints and providing individuals with information on UCCS *designated health care components* practices. The UCCS Director of Campus Compliance will sever as the *privacy officer*.
E. Workforce Training and Management. UCCS *designated health care components* shall train all *workforce members* on its privacy policies and procedures, as necessary and appropriate for them to carry out their various functions.
F. Sanctions. UCCS and each *designated health care component* shall have and apply appropriate sanctions against *workforce members* who violate its privacy policies and procedures, and/or HIPAA's Privacy and Security Rules.
G. Mitigation. UCCS and each *designated health care component* shall mitigate, to the extent practicable, any harmful effect it learns was caused by its workforce or its *business associates* in violation of its privacy policies and procedures or the HIPAA Privacy Rule.
H. Data Safeguards. UCCS and each *designated health care component* shall maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional uses or disclosures of *PHI* in violation of HIPAA and its own policies, and to limit the incidental uses and disclosures pursuant to otherwise permitted or required uses or disclosures.
I. Complaints**.** UCCS and each *designated health care component* shall establish procedures for individuals to complain about its compliance with its privacy policies and procedures and the Privacy Rule. UCCS *designated health care components* shall explain those procedures in its privacy practices notice.
J. Retaliation and Waiver. UCCS and each *designated health care component* shall not retaliate against a person for exercising rights provided by HIPAA, for assisting in an investigation by the federal or state government or another appropriate authority, or for opposing an act or practice that the person believes in good faith violates any HIPAA standard or requirement. UCCS and each *designated health care component* shall not require an individual to waive any right under HIPAA as a condition for obtaining treatment, payment, and enrollment or benefits eligibility.
K. Documentation and Record Retention. UCCS and each *designated health care component* shall maintain, until at least six years after the later of the date of their creation or last effective date, its privacy policies and procedures, its privacy practices notices, dispositions of complaints, and other actions, activities, and designations that the Privacy Rule requires it to be documented.
L. Attachments. The attachments in section IV of this policy may be amended as needed with written approval from the UCCS *privacy officer*, the UCCS *security officer,* and the Vice Chancellor responsible for compliance.

III. KEYWORDS

A. *Business Associate:* a person or entity that creates, receives, maintains or transmits *PHI* to perform certain functions or activities on behalf of a *CE* or provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services for a *CE* and the provision of the service involves the disclosure of *PHI*. 45 C.F.R. § 160.103. All *Business Associate Agreements* (BAAs) not in the template format must be reviewed by the UCCS *privacy officer* and the Office of University Counsel. Any breach of a BAA must be reported as soon as possible to the UCCS *privacy officer*.

B. *Covered Entity (CE):* a health plan, a health care clearinghouse or a health care provider who transmits any *health information* in electronic form in connection with a covered transaction. 45 C.F.R. § 160.103

C. *Covered Transaction:* the transmission of information between two parties to carry out financial or administrative activities related to health care and includes the following transmissions:
    1. Health care claims or equivalent encounter information.
    2. Health care payment and remittance advice.
    3. Coordination of benefits.
    4. Health care claim status.
    5. Enrollment and disenrollment in a health plan.
    6. Eligibility for a health plan.
    7. Health plan premium payments.
    8. Referral certification and authorization.
    9. First report of injury.
    10. Health claims attachments.
    11. Health care electronic funds transfers (EFT) and remittance advice.
    12. Other transactions that the Secretary may prescribe by regulation. 45 C.F.R. § 160.103

D. *Data Use Agreement (DUA):* UCCS *designated health care components* may use or disclose a *limited data set (LDS)* only if it obtains satisfactory assurance, in the form of a written *DUA*, that the *LDS* recipient will use or disclose the *PHI* for limited purposes. If the *UCCS DUA template* is not used, then the following components must be included in the agreement:
    1. Establish the permitted uses and disclosures of the *LDS*, which must be limited to the purposes of *research*, public health, or *health care operations*;
    2. Limit the *LDS* recipient to use or further disclose the *PHI* in the manner that the UCCS *designated health care component* may allow;
    3. Establish who is permitted to use or receive the *LDS*;
    4. Provide that the *LDS* recipient will:
        a. Not use or further disclose the *PHI* other than as permitted by the agreement or as otherwise required by law;
        b. Use appropriate safeguards to prevent use or disclosure of the *PHI*, other than as provided for by the agreement;
        c. Report to the UCCS *privacy officer* any improper use or disclosure of the *LDS* not provided for by the agreement of which the *LDS* recipient becomes aware;
        d. Ensure that any agents, including a subcontractor, to whom it provides the *LDS* agrees to the same restrictions and conditions that apply to the *LDS* recipient with respect to such *PHI*; and
        e. Not identify the *PHI* or contact the patients.
    5. State that if the UCCS *designated health care component* becomes aware of a pattern of activity or practice of the *LDS* recipient that constitutes a material breach or violation of agreement, the UCCS *designated health care component* must take reasonable steps to cure the *breach* or end the violation, as applicable. If such steps are unsuccessful, the UCCS *designated health care component* must:
        a. Discontinue disclosure of the *LDS* to the recipient; and

b. Report the problem to the Secretary of the Department of Health and Human Services.

All *DUA's* not in the template format must be reviewed by the UCCS *privacy officer* and the Office of University Counsel. Any breach of a *DUA* must be reported as soon as possible to the UCCS *privacy officer*.

E. *Designated Health Care Components*: As a *hybrid entity*, the applicable HIPAA compliance obligations apply only to the University's *designated health care components*.
   1. The *designated health care components* include:
      a. Any component that meets the definition of *CE* if it were a separate legal entity;
      b. Components only to the extent that they perform covered functions; and
      c. Components that provide *business associate* services to components that perform covered functions.
   2. The *designated health care components* for UCCS can be found in Exhibit A of APS 5055 HIPAA Hybrid Entity Designation.
   3. Employee and Information Services, in consultation with the Office of University Counsel, shall review and amend Exhibit A as needed, but no less frequently than annually.

F. *Designated Record Set:* A group of records maintained by a UCCS *designated health care component* that is the medical and billing records about an individual and is used in whole or in part by the UCCS *designated health care component* to make decisions about the individual.

G. *Electronic protected health information (ePHI):* refers to any *PHI* that is covered under Health Insurance Portability and Accountability Act of 1996 (HIPAA) security regulations and is produced, saved, transferred or received in an electronic form.

H. *Health Care Component:* A unit or combination of units designated by UCCS because they meet the definition of *CE* or *business associate* in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) including all pertinent regulations (45 CFR Parts 160 and 164) issued by the U.S. Department of Health and Human Services as either have been amended by Subtitle D of the Health Information Technology for Economic and Clinical Health Act (the "HITECH" Act), as Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5). This definition also includes the UCCS Health Circle Clinics and any other UCCS unit that falls within the definition of a *business associate* of the UCCS HealthCircle Clinics. UCCS *health care components* are identified in Exhibit A of APS 5055 HIPAA Hybrid Entity Designation.

I. *Health Care Operations:* Include but are not limited to the following activities:
   1. Quality assessment and improvement activities including:
      a. Outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of studies resulting from such activities;
      b. Patient safety activities;
      c. Population-based activities relating to improving health or reducing health care costs; protocol development; case management and care coordination; contacting of health care providers and patients with information about treatment alternatives;
   2. Reviewing the competence or qualifications of health care professionals;
   3. Evaluating practitioner and provider performance;
   4. Conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or to improve their skills as health care providers;
   5. Training of non-health care professionals;
   6. Accreditation, certification, licensing, or credentialing activities;
   7. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
   8. Business planning and development;
   9. Business management and general administrative activities of the UCCS *designated health care components*, including, but not limited to, management activities related to implementation of

and compliance with HIPAA requirements, resolution of internal grievances, creating de-identified *health information* or a *limited data set*, and fundraising for the benefit of the UCCS *designated health care component*.

J. *Health Information*: Information created or received by a health care provider, health plan, public health authority, employer, life insurer, school, university, or health care clearinghouse that relates to: an individual's past, present or future physical or mental health or condition; the provision of health care to an individual; or payment for provision of health care to an individual.

K. *HIPAA-Related Documentation*: Documentation that contains *protected heath information (PHI)* or is required by UCCS HIPAA policies.

L. *Hybrid Entity:* A single legal entity that conducts both covered and non-covered functions and designates *health care components* in accordance with 45 C.F.R. § 164.105(a)(2)(iii)(D). 45 C.F.R. § 164.103

M. *Incidental Disclosure***:** A secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and occurs as a result of another use or disclosure that is permitted by the Rule.

N. *Limited Data Set (LDS):* Use or disclose *limited data sets* of *PHI* without the need for a valid authorization for the purpose of *research*, public health, or *health care operations*, as long as the following conditions are met;

1. That the purpose of the use and disclosure is limited to *research*, public health, or *health care operations*;
2. That the use or disclosure complies with the *Minimum Necessary Standard*;
3. The source of the *PHI* and the use or disclosure does not place an undue burden on UCCS *designated health care component* resources.

An *LDS* consists of *PHI* that excludes the following identifiers of the individual, or of the individual's relatives, employers, or household members:

1. Names;
2. Postal address information, other than town and city, State, and zip code;
3. Telephone numbers;
4. Fax numbers;
5. Electronic mail addresses;
6. Social security numbers;
7. Medical record numbers;
8. Health plan beneficiary numbers;
9. Account numbers;
10. Certificate/license numbers;
11. Vehicle identifiers and serial numbers, including license plate numbers;
12. Device identifiers and serial numbers;
13. Web Universal Resource Locators (URLs);
14. Internet Protocol (IP) address numbers;
15. Biometric identifiers, including finger and voice prints; and,
16. Full face photographic images and any comparable images.

Before an *LDS* may be disclosed, a *data use agreement* must be in place between UCCS and the recipient of the *LDS*.

O. *Minimum Necessary Standard:* Applies when using or disclosing *PHI*, or when requesting *PHI* from others. A *CE* must take reasonable steps to limit uses and disclosures of *PHI* to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. The *minimum necessary standard* applies to all uses and disclosures for the purposes of payment, *health care operations,* and *research* (it does not apply to treatment). Even if accessing *PHI* for *research* purposes pursuant to an authorization, the researcher must limit the amount of information requested in the authorization to the minimum necessary.

P. *Privacy Board*: A review body that may be established to act upon requests for a waiver or an alteration of the authorization requirement under the Privacy Rule for uses and disclosures of *PHI* for a particular

research study. A *privacy board* may waive or alter all or part of the authorization requirements for a specified research project or protocol. A *CE* may use and disclose *PHI*, without an authorization or with an altered authorization, if it receives the proper documentation of approval of such alteration or waiver from a *privacy board*.

Q. *Privacy Officer:* is the UCCS Director of Campus Compliance who is responsible for managing the risks and business impacts of HIPAA privacy laws and policies. For detailed information, visit the Ethics and Compliance Website at https://www.uccs.edu/compliance/ or contact directly at comply@uccs.edu.

R. *Protected Health Information (PHI):* means individually identifiable *health information* transmitted or maintained in any form or medium that is created, collected, or received by the UCCS *designated health care components*, whether used for academic, administrative, *research* or health care purposes. *PHI* excludes individually identifiable *health information* in education records covered by Family Educational Rights and Privacy Act (FERPA) and in University employment records. The following are identifiers of the individual or of relatives, employers, or household members of the individual:

1. Names;
2. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
   a. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
   b. The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
   c. Currently, 036, 059, 063, 102, 203, 556, 592, 790, 821, 823, 830, 831, 878, 879, 884, 890, and 893 are all recorded as "000".
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. Telephone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Social security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code,

The *CE* does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

S. *Research***:** A systematic investigation designed to develop or contribute to generalizable knowledge. (As defined by the National Institute of Health)

T. *Security Incident***:** means an attempted or successful acquisition, unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system, in a manner not permitted under the HIPAA Security Rule (45 CFR Part 160 and 164, Subpart C) which compromises the security or privacy of *ePHI*.

U. *Security Officer*: The UCCS information security officer who is responsible for the ongoing management of information security policies, procedures, and technical systems in order to maintain the confidentiality, integrity, and availability of all organizational healthcare information systems.

V. *Workforce Member:* As defined by the Privacy Rule, includes an employee, volunteer, trainee, contractor and other person whose conduct, in the performance of work for a UCCS *designated health care component*, is under the direct control of the University, whether or not paid by the University.

IV. RELATED POLICIES, PROCEDURES, FORMS, GUIDELINES, AND OTHER RESOURCES

A. Administrative Policy Statements (APS) and Other Policies
   1. APS 2006 Retention of University Records
   2. APS 2027 Code of Conduct
   3. APS 5055 HIPAA Hybrid Entity Designation
   4. APS 6002 Electronic Communications
   5. APS 6005 IT Security Program
   6. APS 6010 Data Governance
   7. Reporting and filing a complaint (see Compliance and Ethics Website)
   8. UCCS Policy 100-001 Campus Policy Process
   9. UCCS Policy 700-001 E-Mail as Official Means of Communication
   10. UCCS Policy 700-003 Information Technology Security
   11. UCCS Policy 700-004 Wireless Networks
   12. UCCS Policy 700-005 Computer Security Incident Response
   13. UCCS Policy 700-006 Computer and Electronics Disposal
   14. UCCS Policy 800-002 Social Media Policy

B. Procedures

C. Forms

D. Guidelines

E. Other Resources (i.e. training, secondary contact information)
   1. American Recovery and Reinvestment Act ("ARRA")
   2. Health Insurance Portability and Accountability Act ("HIPAA")
   3. Health Information Technology for Economic and Clinical Health ("HITECH")
   4. National Institute of Technology ("NIST")

F. Frequently Asked Questions

V. HISTORY

Initial Policy approval	April 19, 2004
Revised	February 20, 1995
Revised	February 1, 2018
Reviewed/Certified	January 17, 2023

VI. APPENDICES

Attachment Number	Name	Reference	Brief Overview
1	**Policies and Procedures Policy** General Requirement	164.306; 164.316 164.312(b)(1) 164.530(i)	Implement reasonable and appropriate P&Ps to comply with all standards, implementation specifications, or other requirements. P&P changes must be appropriately documented.
2	**HIPAA Documentation Policy (Retention)** Requirement	164.530(j)(1)(ii) 164.530(j)(1)(iii) 164.312(b)(2) 164.316	Maintain all P&Ps in written (may be electronic) form. If an action, activity or assessment must be documented, maintain written (may be electronic) records of all. Retain all required documentation for 6 years from the date of its creation or the date when it last was in effect, whichever is later.
3	**HIPAA Documentation Availability and Updating**	164.310 164.316 164.530(j)	Make documentation available to those persons responsible for implementing the Policies and/or Procedures to which the documentation pertains.

Attachment Number	Name	Reference	Brief Overview
	Policy Requirement		Review documentation periodically and update as needed, in response to environmental or operational changes affecting the security of PHI.
4	HIPAA Investigations Policy	160.308 164.310 164.312	CEs and BAs must implement policies & procedures to assure compliance with HHS investigation & recordkeeping requirements.
5	Breach Notification Policy	164.400 to 164.414	Requires CEs and BAs to comply with all Breach Notification requirements: risk analysis; determination of potential harm; notifications.
6	HIPAA Training Policy	164.530(b)	CEs and BAs must train all affected workforce members on their Policies & Procedures, as well as the basics of HIPAA, as needed.
7	Patient Rights Policy	164.520 to 164.528	CEs (and BAs optionally) must implement policies & procedures to assure the lawful provision of Patient Rights as called for in HIPAA regulations
8	PHI Uses and Disclosures Policy	164.502 to 164.514	CEs and BAs must establish methods and procedures to assure that all PHI uses & disclosures are in accord with HIPAA regulations
9	Use and Disclosure for Research Purposes	164.508 164.512 (i) 164.514 (e)	CEs and BAs must establish methods and procedures to assure that all PHI uses & disclosures related to research are in accord with HIPAA regulations
10	Privacy Complaints Policy	164.530(d) 164.530(a)	CEs and BAs must establish methods and procedures to assure the proper handling of, and response to, all complaints received.
11	Risk Management and Risk Analysis Policy Required Standard	164.302 to 164.318 164.308(a)(1)	Establishes the overall Risk Management process that CEs and BAs must implement to meet Privacy & Security Rule compliance requirements. Conduct assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the entity. Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Sec. 164.306(a).
12	Sanction Policy Required Standard	164.308(a)(1)	Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.
13	Information System Activity Review Required Standard / Authorization and Supervision Policy Addressable Standard / Log-in Monitoring Policy Addressable Standard	164.308(a)(1) 164.308(a)(3) 164.308(a)(5)	Implement procedures to regularly review information system activity: audit logs; access reports; and security incident reports; etc. Implement procedures for authorization and/or supervision of workers who work with ePHI or in locations where it might be accessed. Implement Procedures for monitoring and reporting log-in attempts and discrepancies.
14	Workforce Clearance and Access/Termination Policy Addressable Standard	164.308(a)(3) 164.308(a)(4) 164.308(a)(3)	Implement procedures to determine that the access of a workforce member to ePHI is appropriate, including for workstations, transactions, programs, processes, or other mechanisms. Implement procedures for terminating access to ePHI when the employment ends or as required by (a)(3)(ii)(B) of this section.
15	HIPAA Security Reminders Policy Addressable Standard	164.308(a)(5)	Implement periodic reminders of security and information safety best practices.
16	HIPAA Malware Protection Policy Addressable Standard	164.308(a)(5)	Implement Procedures for guarding against, detecting, and reporting malicious software.
17	HIPAA Password Management Policy Addressable Standard	164.308(a)(5)	Implement Procedures for creating, changing, and safeguarding appropriate passwords.

Attachment Number	Name	Reference	Brief Overview
18	HIPAA Security Incident Policy Required Standard	164.308(a)(6) 164.400 to 164.414	Identify and respond to suspected or known security incidents. Mitigate harmful effects. Document security incidents and their outcomes.
19	HIPAA Data Backup Policy Required Standard Data Backup and Storage Policy Addressable Standard	164.308(a)(7) 164.310(d)(1-2) 164.308(a)(7)	Establish and implement procedures to create and maintain retrievable, exact copies of ePHI during unexpected negative events. The Data Backup Plan defines what data is essential for continuity after damage or destruction of data, hardware, or software. Risk Analysis determines what to backup.
20	HIPAA Disaster Recovery Policy Required Standard	164.308(a)(7)	Establish (and implement as needed) procedures to restore any loss of data.
21	Emergency Mode Operations Policy Required Standard	164.308(a)(7)	Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of ePHI while operating in emergency mode.
22	Policy on Testing and Revision of Contingency and Emergency Plans and Procedures Addressable Standard	164.308(a)(7)	Implement procedures for periodic testing and revision of contingency and emergency plans.
23	Policy on Applications and Data Criticality Analysis Addressable Standard	164.308(a)(7)	Assess the relative criticality of specific applications and data in support of other contingency plan components.
24	Policy on Evaluating the Effectiveness of Security Policies and Procedures Required Standard	164.308(a)(8)	Perform periodic technical & nontechnical evaluations, to establish how well security P&Ps meet the requirements of this subpart.
25	Business Associates Policy Required Standard	164.308(b)(1) 164.410 164.502(e) 164.504(e)	CE's must obtain, and BA's must provide, written satisfactory assurances that all ePHI and PHI will be appropriately safeguarded.
26	Contingency Operations Policy Addressable Standard	164.310(a)(1-2)	Establish (and implement as needed) procedures that allow facility access to support restoration of lost data in the event of an emergency.
27	Facility Security Policy Addressable Standard	164.310(a)(1-2)	Implement P&P's to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
28	Access Control and Validation Policy Addressable Standard	164.310(a)(1-2)	Implement procedures to control and validate individual access to facilities based on role or function; including visitor control, and access control for software testing and revision.
29	Maintenance Records Addressable Standard	164.310(a)(1-2)	Implement P&Ps to document repairs and changes to physical elements of a facility related to security (hardware, walls, doors, locks, etc.).
30	Workstation Use and Security Policy Required Standard	164.310(b-c)	Implement P&Ps that specify the proper functions, procedures, and appropriate environments of workstations that access ePHI. Implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.
31	Media Disposal and Re-Use Required Standard	164.310(d)(1-2)	Implement P&Ps to address the final disposition of ePHI, and/or the hardware or electronic media on which it is stored.

Attachment Number	Name	Reference	Brief Overview
	/Hardware and Media Accountability Policy Addressable Standard		Implement procedures for removal of ePHI from electronic media before the media are made available for re-use. Maintain records of the movements of hardware and electronic media, and any person responsible therefore.
32	Unique User Identification Policy Required Standard	164.306 164.312(a)(1-2)	Assign a unique name and/or number for identifying and tracking user identity.
33	Emergency Access Policy Required Standard	164.104 164.306 164.312(a)(1)	Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.
34	Automatic Log-Off Policy Addressable Standard	164.306 164.312(a)(1-2)	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
35	Encryption and Decryption Policy Addressable Standard	164.312(a)(1-2)	Implement an appropriate mechanism to encrypt and decrypt ePHI.
36	Audit Controls Policy Required Standard	164.312(b)	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.
37	Data Integrity Controls Policy Addressable Standard	164.312(c)(1-2)	Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.
38	Person or Entity Authentication Policy Required Standard	164.312(d)	Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.
39	Data Transmission Security Policy Addressable Standard	164.312(e)(1)	Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.

VII.FORMS

Form Number	Name	Reference	Corresponding Attachment
1	Business Associates Agreement Template	164.308(b)(1) 164.410 164.502(e) 164.504(e)	HIPAA Compliance Policy Attachment 5 Breach Notification
2	Authorization to Release and or Obtain Patient Information	164.502 to 164.514	Attachment 7 Patient Rights Policy Attachment 8 PHI Uses and Disclosures Policy
3	HIPAA Authorization for Release of Health Information – Media	164.502 to 164.514	Attachment 8 PHI Uses and Disclosures Policy
4	Authorization to Use or Disclose Identifiable Health Information for Research	164.508 164.512 (i)	Attachment 9 Use and Disclosure for Research Purposes

5	Request for Waiver of Elements of Authorization or an Altered Authorization	164.508 164.512 (i)	Attachment 9 Use and Disclosure for Research Purposes
6	Activities Preparatory to Research Request for Waiver Form	164.508 164.512 (i)	Attachment 9 Use and Disclosure for Research Purposes
7	Required Representations for Research on Decedents Information Form	164.508 164.512 (i)	Attachment 9 Use and Disclosure for Research Purposes
8	Data Use Agreement		Attachment 8 PHI Uses and Disclosures Policy Attachment 9 Use and Disclosure for Research Purposes
9	Notices of Privacy Practices	164.502 to 164.514	Attachment 7 Patient Rights Policy Attachment 8 PHI Uses and Disclosures Policy
10	Privacy Complaint Form	164.530(d) 164.530(a)	Attachment 7 Patient Rights Policy Attachment 10 Privacy Complaints Policy
11	Privacy - Security Incident Report	164.502 to 164.514	
12	Revocation of Authorization	164.502 to 164.514	Attachment 8 PHI Uses and Disclosures Policy Attachment 9 Use and Disclosure for Research Purposes
13	Request for Accounting of Disclosures of Protected Health Information	164.502 to 164.514	Attachment 7 Patient Rights Policy
14	Request for Amendment of Health Information	164.502 to 164.514	Attachment 7 Patient Rights Policy
15	Approval of Request to Amend Medical or Billing Records	164.502 to 164.514	Attachment 7 Patient Rights Policy
16	Denial of Request to Amend Healthcare Information	164.502 to 164.514	Attachment 7 Patient Rights Policy
17	Request to Restrict Uses or Disclosures of Personal Medical Records	164.502 to 164.514	Attachment 7 Patient Rights Policy
18	Request for Alternate Means of Communication of Confidential Medical Information	164.502 to 164.514	Attachment 7 Patient Rights Policy
19	Request to View or Obtain Copy of Personal Medical Records	164.502 to 164.514	Attachment 7 Patient Rights Policy
20	PHI Disclosure Accounting Log	164.502 to 164.514	Attachment 8 PHI Uses and Disclosures Policy

21	**HIPAA Walkthrough Checklist**	164.502 to 164.514	Attachment 11 Risk Management and Risk Analysis Policy
22	**HIPAA Security Workbook**	164.502 to 164.514	Attachment 11 Risk Management and Risk Analysis Policy

**Note: Forms may change without notice. Please obtain the most current form from the Ethics and Compliance Website at https://www.uccs.edu/compliance/news/health-insurance-portability-and-accountability-act-1996-hipaa.*

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

Policies and Procedures Policy
Attachment 1

Scope of Policy

This policy governs the establishment and maintenance of policies and procedures for UCCS and its *designated healthcare components*. All *workforce members* of UCCS *designated health care components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated health care components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

1. The University Administrative Policy Statement designates which UCCS components are *designated health care components* as per Exhibit A in the APS 5055 HIPAA Hybrid Entity Designation.
2. It is the Policy of UCCS to develop and implement written privacy and security policies and procedures that are consistent with the HIPAA rules and the UCCS Policy 100-001 Campus Policy Process. If necessary, the UCCS healthcare component leadership will develop department/unit level policies and procedures.
3. All UCCS *designated health care components* policies and procedures shall be updated and amended as needed or as required by law and as suggested by good business practices and general business ethics.
4. All UCCS *designated health care components* policies and procedures shall be distributed to, or made otherwise available to, the entire workforce.
5. All UCCS *designated health care components* policies and procedures shall be regularly maintained and secured, and copies shall be stored offsite with other important business records for safekeeping.
6. All members of the workforce are required to read, understand, and comply with this and all other policies and procedures created and implemented by the UCCS and its *designated health care components*.

Procedures

1. UCCS shall create or revise its own HIPAA policies and procedures, consistent with all applicable HIPAA rules and regulations as well as with applicable state laws and statutes.
2. The UCCS *privacy officer* and UCCS *security officer* will assume control of the campus HIPAA policies and procedures process.
3. Legal counsel will be included to guide or review the policies and procedures creation/revision process and to intercede where necessary to ensure UCCS HIPAA policies and procedures meet all applicable HIPAA (and other) standards.

4. UCCS shall internally publish its HIPAA policies and procedures, when complete, to its *workforce members* and shall provide appropriate training to members of its workforce on the interpretation and implementation of its policies and procedures.
5. Each director/designate of UCCS *designated health care components* shall create or revise its own policies and procedures to ensure compliance with the UCCS HIPAA policies and procedures.
6. Each director/designate of UCCS *designated health care components* shall maintain documentation on training of workforce related to the all HIPAA policies and procedures.

Related Policies

APS 5055 HIPAA Hybrid Entity Designation
UCCS Policy 100-001 Campus Policy Process

Reference

45 CFR § 164.316
45 CFR § 164.306(b)(2)(i), (ii), (iii), and (iv)

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

HIPAA-Related Documentation Policy (Retention)
Attachment 2

Scope of Policy

This policy governs the creation and maintenance of *HIPAA-related documentation* for UCCS and its *designated health care components*. All *workforce members* of UCCS *designated health care components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, b*usiness associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated health care components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

1. Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated health care components* who work for or perform any services (paid or unpaid) must document all HIPAA-related activities that require documentation.
2. All *HIPAA-related documentation* must be created and maintained in written form, which may also include electronic forms of documentation.
3. *HIPAA-related documentation* shall be securely stored and maintained in a manner consistent with the HIPAA Privacy and Security Rule Standards.
4. Any action, activity or assessment that must be documented, shall be documented in accordance with this and other policies and procedures implemented by the University and its *designated health care components*.
5. All *HIPAA-related documentation* must be forwarded, used, applied, filed, or stored in accordance with this and other policies and procedures created and implemented by the University and its *designated health care components*.
6. All required *HIPAA-related documentation* shall be securely and appropriately maintained and stored in accordance with HIPAA regulations and with the University, campus, and HIPAA policies on document retention.
7. It is the Policy of the university to retain all *HIPAA-related documentation* for a minimum period of six (6) years from the date of its creation or modification, or the date when it was last in effect, whichever is later.
8. *HIPAA-related documentation* shall be made available to those *workforce members* who have a legitimate need for it, and who are authorized to access it, according to current HIPAA standards.

Procedures

1. Each UCCS *designated health care component* is responsible for developing and maintaining departmental policies and procedures related to their documentation requirements and retention.

2. Each UCCS *designated health care component* is responsible for maintaining documentation of their workforce training and education related to HIPAA (no less than six years).

Related Polices

APS 2006 Retention of University Records
UCCS Retention Schedule

Reference

45 CFR § 164.316
45 CFR § 164.530(j)(ii),(iii),
45 CFR § 164.312(b)(2)

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

HIPAA-Related Documentation Availability and Updating Policy
Attachment 3

Scope of Policy

This policy governs *HIPAA-related documentation* availability and updating for UCCS and its *designated health care components*. All *workforce members* of UCCS *designated health care components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated health care components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

1. It is the Policy of UCCS and its *designated health care components* to make all *HIPAA-related documentation* available to those persons responsible for implementing the policies and/or procedures to which such documentation pertains.
2. All *HIPAA-related documentation* shall be distributed or made otherwise available to all *workforce members* who are affected by the documentation, or who require such documentation in the performance of their work-related duties.
3. *Workforce members* affected by specific *HIPAA-related documentation* shall have access to such documentation prior to their beginning or executing work that depends on such documentation.
4. No member of the workforce shall be held accountable for compliance with any *HIPAA-related documentation*, policies, or procedures unless they have access to such documentation.
5. It is the Policy of UCCS and its *designated health care components* to review all *HIPAA-related documentation* periodically, and update such documentation as needed, in response to environmental or operation changes affecting the privacy or security of individually identifiable *health information*.
6. Reviews of *HIPAA-related documentation* shall be made periodically, but at least annually, for the purposes of this policy.
7. Campus-wide reviews and updates of *HIPAA-related documentation* that occur as a result of this policy shall be made by the UCCS *privacy officer* or the UCCS *security officer.*
8. Department-specific reviews and updates of *HIPAA-related documentation* that occur as a result of this policy shall be made by UCCS *designated health care components* leadership.

Procedures

1. Each UCCS *designated health care component* is responsible for the education of *workforce members* about documentation requirements for their area.
2. Each UCCS *designated health care component* is responsible for determining if policies and procedures for their area are necessary related to documentation. If it is determined that department-specific policies and procedures are necessary, it is the responsibility of UCCS *designated health care component* leadership to maintain and update those policies and

procedures.

Related Polices

APS 6001 Providing and Using Information Technology
APS 6005 IT Security Program
APS 6010 Data Governance
Principals of Ethical Behavior
UCCS Policy 700-002 Responsible Computing
UCCS Policy 700-003 Information Technology Security

Reference

45 CFR § 164.310
45 CFR § 164.316
45 CFR § 164.530(j)

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

HIPAA Investigations Policy
Attachment 4

Scope of Policy

This policy governs HIPAA investigations for UCCS *designated health care components*. All *workforce members* of the UCCS *designated health care components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated health care components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

1. It is the Policy of the University and UCCS *designated health care components* to fully comply with HIPAA law and with all HIPAA-related investigations conducted by Health & Human Services (HHS).
2. It is the Policy of the University and UCCS *designated health care components* to not impede or obstruct any HIPAA-related investigations conducted by HHS.
3. It is the Policy of the University and UCCS *designated health care components* to provide all documentation or assistance required by law in connection with any HIPAA-related investigations conducted by HHS.

Procedures

Workforce members who are designated to assist with HIPAA-related investigations conducted by HHS must adhere to the following procedures:

1. Whenever a HHS investigation is discovered, the following persons must be immediately notified:
   A. Chancellor
   B. Privacy officer
   C. Security officer
   D. Office of University Counsel
   E. UCCS *designated health care component's* leadership
2. Ask for the official government agency-issued identification of the investigators (business cards are NOT official identification); write down their names, office addresses, telephone numbers, fax numbers, and e-mail addresses. If investigators cannot produce acceptable I.D., call legal counsel immediately.
3. Cooperate, but do not volunteer information or records that are not requested.
4. Have at least one, if not two, witnesses available to testify as to your requests and their responses.
5. Ask for the name and telephone number of the lead investigator's supervisor, but only if, in your judgment, his/her demeanor indicates that you can ask such a question without engendering

"hard feelings." Under NO circumstances should you take any action to escalate tensions, except if you genuinely doubt the identity or authority of the investigators.

6. Determine if there are any law enforcement personnel present (i.e., FBI, US Attorney investigators, State Prosecutor investigators, etc.). If law enforcement personnel are present, then the investigation is likely a criminal one, with much more severe penalties than may result from a civil investigation. If in doubt, ask.
7. Permit the investigators to have access to *protected health information (PHI)* in accordance with our Notice of Privacy Practices form (NPP) and Federal and State law. Once investigators have verified their identities and have also verified their authority to access *PHI*, it is a violation of HIPAA to withhold *PHI* from them if the *PHI* sought is the subject matter of the investigation or reasonably related to the investigation. Again, ask investigators to verify that they are seeking access to the information because it is directly related to their legitimate investigatory purposes; and document their responses in your own written records.
8. Have a witness with you when you ask about their authority to access *PHI*, and the use that they will make of the *PHI* they are seeking access to, who can later testify as to what they told you. Two witnesses are even better. All witnesses should also prepare a written summary of the conduct and communications they observed as soon as possible after the incident; these summaries should be annotated with the time and date of the event, the time and date that the summaries were completed, and the witnesses signature. A copy of the summary should be sent to the UCCS *privacy officer*.
9. Send staff employees elsewhere, if possible, during this first investigation encounter. There is no requirement that we provide witnesses to be questioned during the initial phase of an investigation.
10. Do NOT instruct employees to hide or conceal facts, or otherwise mislead investigators.
11. Ask the investigators for documents related to the investigation. For example, request:
    A. copies of any search warrants and/or entry and inspection orders
    B. copies of any complaints
    C. a list of patients they are interested in
    D. a list of documents/items seized
12. Do NOT expect that investigators will provide any of the above, except for the search warrant and a list of documents/items seized (if any).
13. Do not leave the investigators alone, if possible. Assign someone to "assist" each investigator present.
14. Do not offer food (coffee, if already prepared, and water, if already available, is ok). Don't do anything that could be construed as a "bribe" or a "kickback" to induce favorable treatment, such as offering to buy the investigators lunch.
15. Tell investigators what you are required by law to tell them. Answer direct questions fully and to the best of your ability. Always defer to the advice of legal counsel if you are unsure of what or how much to say.

Related Polices

APS 2027 Code of Conduct
Principals of Ethical Behavior

Reference

45 CFR § 160.308
45 CFR § 164.310

45 CFR § 164.312

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

Breach Notification Policy
Attachment 5

Scope of Policy

This policy governs breach notification for UCCS and its *designated health care components*. All *workforce members* of the UCCS *designated health care components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated health care components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

1. It is the Policy of the University, UCCS, and its *designated health care components* to provide timely notifications to affected patients/clients or consumers about *breaches* of individually identifiable *health information*.
2. UCCS *designated health care components*, in conjunction with the UCCS *privacy officer* and legal counsel, shall notify individuals when a *breach* is discovered. A *breach* is treated as "discovered" by the University the first day on which such *breach* is known or should reasonably have been known to any *workforce member* of the UCCS *designated health care component*, other than the person who committed the *breach*.
3. Notification must occur without unreasonable delay and in no event later than 60 days from discovery of the *breach*, unless law enforcement requests a delay.

Procedures

1. *Breach* notices must include, at a minimum, a brief description of what happened, a description of the types of *protected health information (PHI)* involved, steps the individual should take to protect themselves from potential harm, a brief description of the actions taken in response to the breach, and contact procedures for the individual to ask questions.
2. First class mail shall be the default method of notification. The University may use e-mail if requested by the individual, or substitute notice via the University website or local print or broadcast media if we do not have current contact information.
3. The University must notify major local media outlets of a *breach* affecting more than500 individuals.
4. *Business associates* of the University are required to immediately report all *breaches*, losses, or compromises of individually identifiable *health information* – whether secured or unsecured – to the UCCS *privacy officer*.

5. *Business associate* contracts, whether existing or new, shall have corresponding *breach* notification requirements included in them. Business Associates Agreement Template
6. Sanctions or re-training shall be applied to all *workforce members* who caused or created the conditions that allowed the *breach* to occur, according to Attachment 12 Sanction Policy.
7. All *breach*-related activities and investigations shall be thoroughly and timely documented.

Definitions

As used within the HIPAA Final ("Omnibus") Rule, the following terms have the following meanings:

Breach means the acquisition, access, use, or disclosure of *PHI* in a manner not permitted under federal regulation which compromises the security or privacy of the *PHI*.

1. *Breach* excludes:
   A. Any unintentional acquisition, access, or use of *PHI* by a *workforce member* or person acting under the authority of a *covered entity* or a *business associate*, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under federal regulation of this part.
   B. Any inadvertent disclosure by a person who is authorized to access *PHI* at a *covered entity* or *business associate* to another person authorized to access *PHI* at the same *covered entity* or *business associate*, or organized health care arrangement in which the *covered entity* participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under federal regulation of this part.
   C. A disclosure of *PHI* where a *covered entity* or *business associate* has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.
2. Except as provided in paragraph (1) of this definition, an acquisition, access, use, or disclosure of *PHI* in a manner not permitted under federal regulation is presumed to be a *breach* unless the *covered entity* or *business associate*, as applicable, demonstrates that there is a low probability that the *PHI* has been compromised based on a risk assessment of at least the following factors:
   A. The nature and extent of the *PHI* involved, including the types of identifiers and the likelihood of re-identification;
   B. The unauthorized person who used the *PHI* or to whom the disclosure was made;
   C. Whether the *PHI* was actually acquired or viewed; and
   D. The extent to which the risk to the *PHI* has been mitigated.

Unsecured protected health information means *PHI* that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Pub. L. 111-5.

Reference

45 CFR § 164.400 to 164.41445

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

HIPAA Training Policy
Attachment 6

Scope of Policy

This policy governs HIPAA privacy and security training for the UCCS *designated health care components*. All *workforce members* of UCCS *designated health care components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated health care components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

1. It is the Policy of the University, UCCS, and its *designated health care components* to provide clear and complete HIPAA training to all members of the workforce, including officers, agents, employees, contractors, students, temporary workers, and volunteers.
2. HIPAA training provided by the university shall include relevant and appropriate aspects of both health data privacy and health data security, as it pertains to UCCS and its *designated health care component's* operations and to the duties and responsibilities of specific individuals, workgroups, departments, and divisions.

Procedures

1. HIPAA training, at a minimum, shall include: the basics of HIPAA itself, the basics of HIPAA's privacy and security requirements and restrictions, and a review of relevant and appropriate internal policies and procedures related to HIPAA and HIPAA compliance.
2. HIPAA training shall be provided to all new hires during the new employee orientation period, before new *workforce members* are exposed to or work with individually identifiable *health information*.
3. Each UCCS *designated health care component* shall conduct required HIPAA training periodically for all employees, but no less than annually.
4. Fostering ongoing, continuous HIPAA awareness shall be regarded as a separate type of workforce learning from regular HIPAA training. The UCCS *privacy officer* and the UCCS *security officer*, in conjunction with UCCS *designated health care component* leadership, shall be responsible for the development (or acquisition) and deployment of appropriate HIPAA awareness materials to maintain a high level of HIPAA awareness among the workforce.
5. HIPAA training resources should aim to develop a general understanding of HIPAA and its requirements and restrictions. HIPAA awareness resources should aim to maintain a high level of HIPAA awareness, and a protective attitude toward confidential data on an ongoing, daily basis.
6. It is highly recommended that all *workforce members* take the UCCS HIPAA training module on Skillsoft. For complete instructions on how to access this training please visit the UCCS Ethics

and Compliance Website: https://www.uccs.edu/compliance/news/health-insurance-portability-and-accountability-act-1996-hipaa.

7. UCCS *designated health care component* leadership is responsible for documenting and tracking *workforce members'* training.

Reference

45 CFR § 164.530(b)

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

Patient Rights Policy
Attachment 7

Scope of Policy

This policy governs the provision and management of patient rights for UCCS *designated health care components*. All *workforce members* of UCCS *designated health care components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated health care components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

1. It is the policy of UCCS and its *designated health care components* to provide all of the patient rights to our patients that are called for in the HIPAA regulations. The provision of patient rights in a timely and positive manner can enhance the quality of care we provide to patients, by providing certain rights and controls to patients over their individually identifiable *health information.*
2. Patient rights that the University provides and supports include:
   A. The right to receive a copy of our Notice of Privacy Practices form, which details how individually identifiable *health information* may be used or disclosed by the University (pursuant to section 1 of these procedures).
      B. The right to request restrictions/confidential communications on the use or disclosure of the patient's medical records (pursuant to section 3 of these procedures). Please see Request for Alternate Means of Communication of Confidential Medical Information form.
   B. The right to access or obtain a copy of medical records about the patient (pursuant to section 3 of these procedures), or about the patient's minor children (pursuant to section 4 of these procedures). For specific information about *protected health information (PHI)* disclosures, please see Attachment 8 PHI Uses & Disclosures Policy.
   C. The right to request amendments to medical records, with certain limitations (pursuant to section 5 of these procedures).
   D. The right to an accounting of certain disclosures of individually identifiable *health information* (pursuant to section 6 of these procedures).
   E. The right to file a Privacy Complaint form directly with us, or with the federal government. For specific information about complaints, please see Attachment 10 Privacy Complaints Policy.
3. Each UCCS *designated health care component* shall implement procedures that document and ensure that all patient rights are carried out appropriately.
4. No retaliation of any kind is permitted against any person, patient, or *workforce member* for exercising any right guaranteed by HIPAA.
5. Patient information related to patient rights includes only that information contained in each patient's *designated record set*, which is defined in the HIPAA regulations at § 164.501 as:

A. A group of records maintained by or for a *covered entity* that is:
    1. The medical records and billing records about individuals maintained by or for a covered health care provider;
    2. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
    3. Used, in whole or in part, by or for the *covered entity* to make decisions about individuals.
B. The term "record" means any item, collection, or grouping of information that includes *PHI* and is maintained, collected, used, or disseminated by or for a *covered entity*.

6. It is the policy of UCCS *designated health care components* that the University's *designated record set*, for purposes of fulfilling HIPAA patient rights *includes* the following types or categories of data and items:

Clinical Record	**Source Clinical Data**	**External Records and Reports**
• History and physical • Orders • Progress notes • Lab reports (including contract lab) • Vital signs • Assessments • Consults • Clinical reports • Authorizations and consents • Prescriptions	• X-rays • Images • Fetal strips • Videos • Pathology slides	• External records referenced for patient care: other providers' records, records provided upon transfer • Patient generated records • Personal health records

7. It is the policy of UCCS *designated health care components* that the University's *designated record set*, for purposes of fulfilling HIPAA patient rights *excludes* the following types or categories of data and items:
A. Quality Improvement/Quality Measurement reports and abstracts
B. Statistical data
C. Committee minutes (not patient-specific treatment related)
D. Psychotherapy notes, which are the personal notes of a mental health care provider documenting or analyzing the contents of a counseling session, that are maintained separate from the rest of the patient's medical record. See 45 CFR 164.524(a)(1)(i) and 164.501.
E. Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding. See 45 CFR 164.524(a)(1)(ii).

Procedures

1. Notice of Privacy Practices. A UCCS *designated health care component* that has a direct treatment relationship with an individual must provide the appropriate notice no later than the date of the first occurrence of any form of service delivery including service delivered

electronically provided that: 1) If the first service delivery occurs during an emergency treatment situation then the notice should be delivered as soon as practicable after the treatment; and 2) If the first service delivery occurs electronically, the provider must provide electronic notice automatically and contemporaneously in response to the individual's first request for service.

A. Except in emergency treatment situations, the UCCS *designated health care component* with a direct treatment relationship must make a good faith effort to obtain a written acknowledgement of receipt of notice from the individual.
B. If the individual will not acknowledge receipt of the notice or will not accept the notice, the UCCS *designated health care components* must document good faith efforts to obtain acknowledgement and the reason why the individual would not acknowledge receipt of the notice or would not accept the notice.
C. If the UCCS *designated health care component* maintains a physical service delivery site, the provider must:
    1. Have the notice available at the site for individuals to request to take with them; and
    2. Post the notice in a clear and prominent location.
D. With reference to electronic notice:
    1. The UCCS *designated health care component* must prominently post the notice on its websites and make the notice available electronically through the websites; and
    2. The UCCS *designated health care component* may provide the notice to an individual by e-mail if the individual has agreed to electronic notice and has not withdrawn his or her agreement provided however that:
    3. If the e-mail transmission fails and the failure is known to the insurance plan or provider, then a paper copy of the notice must be provided to the individual; and
    4. The individual who is the recipient of electronic notice retains the right to obtain a paper copy of the notice upon request.
E. Each UCCS *designated health care component* must retain copies of the notices issued by the UCCS *designated health care component* and any written acknowledgments of receipt or efforts made to obtain written acknowledgments. Such documentation must be retained as required by Attachment 2 Documentation Policy (Retention).

2. Right to Request Restrictions/Confidential Communications.
    A. Restrictions.
        1. All requests for restrictions must be made in writing.
        2. UCCS *designated health care components* must agree to a request for a restriction if:
            i. The disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and
            ii. The *PHI* pertains solely to a health care item or service for which the individual or other person (other than a health plan on behalf of the individual) has paid the UCCS *designated health care component* in full.
        3. If a UCCS *designated health care component* does agree to a restriction, the UCCS *designated health care components* must not use or disclose *PHI* in violation of the restriction unless the individual who requested the restriction is in need of emergency treatment and the restricted *PHI* is needed to provide the emergency treatment. In these cases, the UCCS *designated health care components* may use the restricted *PHI* or may disclose the *PHI* to a health care provider to provide emergency treatment to the individual. If the restricted *PHI* is disclosed to a health care provider for emergency treatment, the UCCS *designated health care component* must request that the health care provider who reviews the restricted *PHI* not further use or disclose the information.

4. A restriction agreed to by a UCCS *designated health care component* under this policy is not effective to prevent uses or disclosures of *PHI* required by the Secretary of Health and Human Services or as required or permitted by state or federal law.
5. A UCCS *designated health care component* may terminate its agreement to a restriction if:
    i. The individual agrees to or requests the termination in writing;
    ii. The individual orally agrees to the termination and the oral agreement is documented; or
    iii. The UCCS *designated health care component* informs the individual that it is terminating its prior agreement to a restriction. However, such termination is not effective:
        a. For *PHI* created or received before the individual has been informed of the termination; and
        b. For *PHI* with respect to which the UCCS *designated health care components* must agree to a restriction as described above.

B. Confidential Communications. The following are conditions on receiving and responding to requests for confidential communication of *PHI* by alternative means or at alternative locations:
1. All requests for alternative communications must be submitted to the UCCS *designated health care component* in writing using the Request For Alternate Means of Communication of Confidential Medical Information form. Written requests must include the following information:
    i. The patient's name, date of birth and social security number if required;
    ii. The specific means or alternative locations for contact that are desired;
    iii. What communications of *PHI* are involved; and
    iv. How the patient intends to pay for the costs of the alternative communication.
2. Reasonable means of communication may include but are not limited to: transmission via fax, encrypted e-mail, courier service, or overnight express mail delivery. The individual making the request will be informed of his or her responsibility to pay for any charges incurred.
3. Reasonable alternative locations may include but are not limited to: transmissions of *PHI* to work addresses (physical or electronic), a friend's address (physical or electronic), or post office boxes.
4. All other reasonable requests to have communications of *PHI* sent by specific means or to alternative locations will be granted. An explanation for such requests is not required. A request that no communication of *PHI* be made is not reasonable and will not be granted.
5. Any request for alternative communications that does not include a reasonable means for obtaining payment for the service will be denied.
6. The director/designate of the UCCS *designated health care component* at which the request is being made is authorized to grant requests to receive confidential communications by specific means or at alternate locations.
7. The director/designate of the UCCS *designated health care component* at which the request is being made will inform the individual making the request whether the request is granted or denied. If the request is denied, the individual will be informed of the reason for the denial and, if applicable, any alterations to the request that will allow it to be granted.
8. All requests for alternative communications will be documented in the individual's medical record with a notation of the status of the request and will be maintained permanently in the individual's medical record. If the request does not apply to the

entire medical record, the request will note and identify the specific information that is restricted.

9. If the *PHI* that is subject to the restriction was released to a *business associate*, the *business associate* will be informed of the request for communications by specific means or to alternative locations.
10. If a request is granted, UCCS *designated health care component* personnel must appropriately document the provision of *PHI* by alternative means or at an alternative location and accommodate the request. Such documentation must be retained as required by Attachment 2 Documentation Policy (Retention).

3. Right to access or obtain a copy.
   A. General right. An individual has a right to inspect and/or obtain a copy of *PHI* about the individual in a UCCS *designated health care component*'s *designated record set* (see above), as long as the *PHI* is maintained in the *designated record set*, except for:
      1. Psychotherapy notes, unless approved by the originator of the notes or the successor of the originator;
      2. Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or other legal proceeding, unless otherwise approved by legal counsel;
      3. UCCS *designated health care components*, acting under the direction of a correctional institution may deny access, in whole or part, to an inmate's request to obtain a copy of *PHI*, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the inmate or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible party for the transporting of the inmate.
      4. If the *PHI* was collected during the course of *research* treatment and the individual previously consented to non-access during the term of *research* and was informed that his or her right to access the information would be reinstated upon completion of the *research*. Refer to Attachment 9 Use and Disclosure for Research Purposes.
      5. If the *PHI* was obtained from another person or entity (not a health care provider) under the promise of confidentiality and allowing access would be reasonably likely to reveal the source of the *PHI*.
      6. *PHI* maintained by the UCCS *designated health care component* that is:
         i. Subject to the Clinical Laboratory Improvements Amendments of 1988 ("CLIA") to the extent the provision of access to the individual would be prohibited by law; or
         ii. Exempt from CLIA pursuant to 42 C.F.R. 493.3(a)(2);
   B. Requesting to Inspect and/or to Obtain a Copy.
      1. An individual must request in writing an opportunity to inspect and/or to obtain a copy of his or her *PHI* in a UCCS *designated health care component's designated record set* to any healthcare professional employed by the UCCS *designated health care components*. If the request was not made in writing, the person to whom the request was made must inform the individual of the requirement that requests be in writing. The Authorization to Release and/or Obtain Patient Information form can be used or the Request to View or Obtain Copy of Personal Medical Records form.
      2. All requests to inspect or to obtain a copy of *PHI* will be directed to or submitted by the person receiving the request immediately to the director/designate of the UCCS *designated health care component*.
      3. Upon receipt of a written request, the director/designate of the UCCS *designated health care component* will either permit or deny access. Denials of access must be in writing and must follow the provisions outlined below.

4. All requests for access must be acted on no later than 30 days after receipt of the written request from the patient.
5. The director/designate of the UCCS *designated health care component* should maintain a copy of the completed request form and any documentation relating to any action taken on the request.

C. Granting a Request to Inspect and/or to Obtain a Copy. If the director/designate of the UCCS *designated health care component* grants the request, in whole or in part, he or she must inform the individual of the acceptance of the request and provide the access requested by arranging with the individual for a convenient time and place to inspect the *PHI.* The individual should be provided with access to the *PHI* in the form or format requested by the individual, if reasonable. If the form or format requested is unreasonable, access may be provided by sharing copies of the information with the individual in some other form or format agreed to by both the UCCS *designated health care component* and the individual.
   1. If the individual agrees in advance to receive a summary of the *PHI* requested and to accept the fees, if any, associated with creating a summary, the director/designate of the UCCS *designated health care component* may provide a summary of the *PHI* instead of providing access to the *PHI* itself.
   2. If the individual requests copies of the information, the director/designate of the UCCS *designated health care component* should arrange for the provision of copies within the time limits provided above. The director/designate of the UCCS *designated health care component* should arrange with the individual for a convenient time and place for the individual to pick up the information or for the information to be mailed. The director/designate of the UCCS *designated health care component* may impose a reasonable, cost-based fee for copying and may require reimbursement of the costs of any postage associated with the request.

D. Denial of Access. The UCCS *designated health care component* may deny access under the following circumstances:
   1. A licensed health care provider has determined that access is reasonably likely to endanger the life or physical safety of the patient or another person.
   2. The *PHI* refers to another person (not a health care provider) and a licensed health care professional has determined that access is reasonably likely to cause substantial harm to that person.
   3. The person requesting the *PHI* is the personal representative of the patient and a licensed health care professional has determined that access is reasonably likely to cause substantial harm to the patient or another person.
   4. The patient's access to the *PHI* could be psychologically harmful to the patient.

E. Process for Denial of Access: If a request for access to *PHI* is denied, in whole or in part, the director/designate of the UCCS *designated health care component* must:
   1. To the extent possible, give the individual access to any other *PHI* requested after excluding the *PHI* to which access was denied;
   2. Provide a timely, written denial to the individual which must:
      i. Be in plain language;
      ii. Contain the basis for the denial;
      iii. If applicable, contain a statement of the individual's review rights as provided in paragraph E below, including a description of how the individual may exercise the review rights; and
      iv. Contain a description of how the individual may complain internally about UCCS HIPAA policies and procedures, compliance with HIPAA policies and procedures, or HIPAA compliance in general as described in *Attachment 10 Privacy Complaints Policy.*

3. If the director/designate of the UCCS *designated health care component* has denied the request for access because the UCCS *designated health care component* does not maintain the *PHI* that the individual has requested and the UCCS *designated health care component* knows where the information is maintained, the director/designate of the UCCS *designated health care component* must inform the individual where to direct his or her request for access.

F. Unreviewable Grounds for Denial. The director/designate of the UCCS *designated health care component* may deny an individual access to his or her *PHI* without providing the individual an opportunity for review by the UCCS *privacy officer* or legal counsel in the following circumstances:
   1. The *PHI* is excepted from the right to access pursuant to this policy;
   2. The individual has requested access to *PHI* created or obtained by the UCCS *designated health care component* in the course of *research* that includes treatment, the *research* is in progress, the individual has agreed to a denial of access when consenting to participate in the *research* that includes treatment, and the UCCS *designated health care component* has informed the individual that the right of access will be reinstated upon completion of the *research*;
   3. The individual has requested access to *PHI* that is contained in records that are subject to the Privacy Act, 5 U.S.C. section 552a, and access may be denied under the provisions of the Privacy Act; or
   4. The individual has requested access to *PHI* that was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

G. Reviewable Grounds for Denial. The director/designate of the UCCS *designated health care component* may deny an individual access in the following circumstances:
   1. A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;
   2. The *PHI* makes reference to another person (other than a health care professional) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to the other person; or
   3. The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to the personal representative is reasonably likely to cause substantial harm to the individual or another person.
   4. If access is denied pursuant to this policy, the individual has the right to have the denial reviewed by the UCCS *privacy officer* and legal counsel. Requests for review must be immediately referred to the UCCS *privacy officer*. The reviewing parties must determine within a reasonable period of time whether to grant or deny access. The reviewing parties' determination must be promptly provided to the individual in writing, and the UCCS *designated health care component* must take action to carry out the determination.

4. Privacy Rights of Minors. Although minors do not generally have the authority to exercise rights on their own behalf, state law and the HIPAA Privacy Rule provide minors with the authority to exercise control over certain categories of their own *PHI*.
   A. General. UCCS *designated health care components* will respond appropriately to minors' requests to keep certain categories of their *PHI* confidential and to exercise the rights

granted to patients by the HIPAA Privacy Rule in accordance with state and federal laws and regulations.

B. Minor's Right to Consent to Certain Treatment. A minor may seek and receive the following types of health care services independently from the minor's parent(s) or legal guardian, meaning parental consent is not required:
   1. HIV/AIDS testing and treatment;
   2. Testing and treatment for venereal and sexually transmissible diseases (STDs);
   3. Pregnancy and pre-natal care;
   4. Chemical dependency services (both alcohol and drugs); and
   5. Birth control services. Except where child abuse or neglect are concerned, abortion procedures may not occur until 48 hours after the parent(s) or legal guardian has been notified in writing. However, a minor may elect to not allow notification with a proper court order.

C. Minor's Right to Consent Under Special Circumstances. A minor may seek and receive health care services independently from the minor's parent(s) or legal guardian under the following circumstances:
   1. Emancipated. A minor is emancipated:
      i. By court order, or
      ii. By contracting a lawful marriage, or
      iii. If the minor is 15 years of age or older and is living separate and apart from the minor's parent(s) or legal guardian, with or without the consent of the minor's parent(s) or legal guardian, and is managing the minor's own financial affairs, regardless of the source of the minor's income.
      iv. Emancipated minors may give consent to organ or tissue donation or consent to hospital, medical, dental, emergency health, and surgical care to him/herself.
   2. Mental Health Services. A minor who is 15 years of age or older may independently consent to mental health services but may not necessarily independently consent to disclose the minor's *PHI* in this circumstance. A health care provider may, with or without the consent of the minor, advise the parent(s) or legal guardian of the services given or needed.
   3. Sexual Assault. A minor may consent to medical treatment for sexual assault.
   4. Parent. A minor who is a parent may request and consent to organ or tissue donation of the minor's child or the furnishing of hospital, medical, dental, emergency health, and surgical care to the minor's child or ward.
   5. Abuse. If the health care provider reasonably believes the minor has been or is subject to domestic violence, abuse, and/or neglect, the health care provider must make a reasonable effort to notify the parent(s) or legal guardian before treatment.

D. Except when the minor seeks mental health services, the minor's parent(s) or legal guardian does not have the right to the minor's *PHI* if the minor alone consented to the treatment, unless the minor authorizes the release. Refer to Attachment 8 PHI Uses and Disclosures Policy.

E. Colorado law applies. For example, if a minor whose residence is the state of Texas comes to UCCS's primary care clinic, the laws of the state of Colorado concerning minors apply.

F. Any questions about whether a minor's *PHI* is confidential, or whether access should be made available to the minor's parent(s) or legal guardian, should be directed to the minor's health care provider or the UCCS *privacy officer*.

5. Right to Amend. UCCS *designated health care components* must provide an individual with an opportunity to request that a UCCS *designated health care component* amend *PHI* maintained in the *designated record set*. Except as specifically limited by this policy, individuals will be allowed to amend *PHI* maintained in their medical or billing records.

A. However, amendments may be denied in the following circumstances:
   1. UCCS did not create the record that the individual seeks to amend.
      i. A request for the amendment of *PHI* that was not created by a UCCS *designated health care component* will be considered if the individual submits reasonable evidence of the non-existence or non-availability of the person or facility that created the *PHI*. Such requests will be granted only if they do not fall into another category listed for denial.
   2. A UCCS *designated health care component* does not maintain the information as part of the individual's medical record or *designated record set*.
   3. After reviewing the request and the *PHI* that is the subject of the request, the UCCS *designated health care component* determines that the *PHI* is accurate and complete as recorded in the medical record or *designated record set*.
   4. The *PHI* is the type that would not be available to the individual for inspection. *PHI* not available for inspection includes:
      i. Psychotherapy notes;
      ii. Certain drug and alcohol information;
      iii. *PHI* compiled in anticipation of or for use in civil, criminal or administrative proceedings;
      iv. *PHI* pertaining to participation in ongoing *research* programs, provided the individual previously signed an agreement to forego access to the individual's *PHI* during the term of the study;
      v. *PHI* obtained from someone other than a healthcare provider under a promise of confidentiality, if allowing access would be reasonably likely to reveal the source of the *PHI*;
      vi. *PHI* that is reasonably likely to endanger the life or physical safety of the individual or anyone else;
      vii. *PHI* that makes reference to another person and the individual's (or representative's) access to that *PHI* would be reasonably likely to cause harm to that person;
      viii. *PHI* sought by a representative of the individuals, if access by the representative would cause substantial harm to the individual or another individual.

B. UCCS *designated health care components* will incorporate any amendments to *PHI* made by another *covered entity* if the UCCS *designated health care component* is notified of the amendment and the same *PHI* was also disclosed to the UCCS *designated health care component*.

C. All requests to amend an individual's medical record will be forwarded to the director/designate of the UCCS *designated health care component* in which the record resides.
   1. The director/designate of the UCCS *designated health care component* will handle all inquiries regarding the amendment of *PHI.* Upon request, the director/designate will provide any individual or individual's representative with a Request for Amendment of Health Information form.
   2. Upon receipt of a complete Request for Amendment of Health Information form, the director/designate of the UCCS *designated health care component* will forward the request and the record in question to the originator of the medical record. The director/designate of the UCCS *designated health care component* will ensure the timely receipt of determination. The director/designate will notify the UCCS *privacy officer* when a determination is not made within 60 days of the original request. The originator of the medical record (the "originator") will review the *PHI* in conjunction with the request, consulting with legal counsel as necessary. Within 10 days of receipt of the

request, the originator will submit a preliminary determination to the director/designate, who will review and make a final determination on the request.

3. If the originator of the *PHI* is not available, the amendment will be reviewed by a committee made up of: the director/designate of the UCCS *designated health care component* in which the request is being made; legal counsel; UCCS *privacy officer*; a Chancellor appointee; and other members as deemed necessary. This committee will accept or reject the request for amendment.

D. If the request to amend *PHI* is granted, the Approval of Request to Amend Medical or Billing Records form will be sent to the individual with a copy of the Authorization to Release and or Obtain Patient Information form. A copy of the Approval of Request will be filed in the individual's medical record.

E. If the request to amend *PHI* is denied, a Denial of Request to Amend Healthcare Information form will be sent to the individual. A copy of the Denial of Request will be filed in the individual's medical record.

F. If the individual replies to the Denial of Request to Amend Healthcare Information, the written rebuttal will be included in the individual's medical record. All future disclosures of the *PHI* at issue will include the rebuttal statement. If the patient requests in writing that the request for amendment be included in all future disclosures of the relevant *PHI*, such requests will also be added to the individual's medical record and all future disclosures will include the request for amendment.

6. Right to Receive an Accounting.

A. Upon written request, the UCCS *designated health care component* shall provide an individual with an accounting pursuant to this policy. The Request for Accounting of Disclosures of Protected Health Information form is available for the individual to complete.

B. UCCS *designated health care components* shall provide an accounting for the following disclosures of *PHI*:

1. To health oversight agencies, see Addendum A to this policy for complete list;
2. For public health activities, see Addendum A to this policy for complete list;
3. For *research*-related treatment;
4. Other disclosures not included as an exception listed below.

C. An accounting will not be provided for the following:

1. Disclosures made for treatment, payment, and healthcare operations;
2. Disclosures made to the individual;
3. Disclosures made for the patient directory;
4. Disclosures made to persons involved in the individual's care including disclosures made to family members;
5. Disclosures made for national security or intelligence purposes;
6. Disclosures to correctional institutions or law enforcement officials in custody of an inmate or suspect;
7. Disclosures made pursuant to an authorization signed by the individual;
8. Disclosures that are part of a *limited data set*;
9. Incidental disclosures as defined by *Minimum Necessary Standards*;
10. Disclosures of de-identified information.

D. An individual is entitled to one accounting per year at no charge. If an individual requests more than one accounting per twelve (12) month period, the individual will be charged a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12 month period.

E. The UCCS *designated health care component* that received a written request for an accounting shall respond to the request within 60 days unless an extension of no more than 30 days is requested.

F. An individual's right to receive an accounting may be suspended for a specified period of time as a result of a request from a health oversight agency or a law enforcement individual.

G. The accounting must include the following information:
   1. All disclosures (not including those excepted from disclosure as described in section IV above) for a 6-year period prior to the receipt of the request, but not before April 14, 2003, including disclosures by or to *business associates*;
   2. Dates of the disclosures;
   3. Recipients with addresses, if known;
   4. Description of the *PHI* disclosed;
   5. Purpose of the disclosure;
   6. For multiple disclosures to the same recipient for the same purpose, the requisite information described above for the first disclosure, the frequency or number of disclosures made, and the date of the last disclosure; and
   7. For disclosures made for a *research* purpose for 50 or more individuals, as described in Attachment 9 Use and Disclosure for Research Purposes: the name of the activity; a description of the activity; a description of the type of *PHI* disclosed; the period during which the disclosures occurred; the name and contact information for the entity and researcher to which the *PHI* was disclosed; and a statement that the *PHI* may or may not have been disclosed for a particular *research* activity. If it is reasonably likely that the *PHI* may have been disclosed for a particular *research* activity and the individual so requests, the UCCS *designated health care component* shall assist the individual in contacting the *research* sponsor and the researcher.

H. The UCCS *designated health care component* must maintain documentation that includes the information required to be included in the accounting, the persons or offices responsible for providing the accounting, and any accounting provided in response to a request.

Reference

45 CFR § 164.520 to 164.528
45 C.F.R. §164.522(a)
C.R.S. § 13-22-102 Minors-consent for medical care and treatment for addiction to or use of drugs
C.R.S. § 13-22-103 Minors-consent for medical, dental, and related care
C.R.S. § 13-22-103.5 Minors-consent for medical care-pregnancy
C.R.S. § 13-22-105 Minors-birth control services rendered by physicians
C.R.S. § 12-37.5-104 Notification concerning abortion
C.R.S. § 12-37.5-107 Judicial Bypass
C.R.S. § 12.37.5-105 No notice required-when.
C.R.S. § 27-10-103 Voluntary applications for mental health services
C.R.S. § 13-22-106 Minors-consent-sexual offense
Planned Parenthood of Rocky Mountains v. Owens, 287 F.3d 910 (10th Cir. 2002)
45 CFR 164.502(g)(3)(i) Un-emancipated minors.

Addendum A: List of Possible PHI Disclosures

Any *protected health information (PHI)* disclosures made under these circumstances or to these agencies must be tracked.

Public Health Authorities

- Surveillance
- Investigations
- Interventions
- Foreign governments collaborating with US public health authorities
- Recording Deaths
- Child Abuse
- Elder Abuse
- Prevent Serious Harm
- Communicable Disease (see Colorado Board of Health's Reportable Diseases below)

Food and Drug Administration

- Adverse events, serious side effects, product defects or biological product deviations
- Track products
- Enable product recalls, repairs, or replacements
- Conduct post marketing surveillance
- Manufactures of defective products

Employer

- To employer requesting healthcare be provided to their employee
- Medical surveillance
- Work related injury or illness
- Occupational Safety and Health Administration (OSHA) regulations or similar state law

Health Oversight

- Government benefit program
- Civil rights laws
- Vital statistics

Judicial and Administrative Proceedings

- Court order
- Subpoena
- Law Enforcement not in custody of an inmate or suspect
- As required by law
- Court order, court ordered warrant, subpoena or summons
- Administrative request
- Locating a suspect, fugitive, material witness or missing person
- Emergency treatment, crime is not on premises
- Victims of crime (for example child and elder abuse, certain wounds incurred with domestic violence)

- Crimes on premises
- Suspicious deaths
- Avert a serious threat to health or safety

Specialized Government Functions
- Military and Veterans activities
- Protective services
- Department of State: Medical Suitability
- Government programs providing public benefits
- Foreign military personnel

Workmen's Compensation
- Comply with Colorado Law

Colorado Department of Public Health & Environment

For the most up-to-date information on communicable and environmental conditions that must be reported to the Colorado Department of Public Health & Environment please click here: https://drive.google.com/file/d/1n-OfQQJMwLTvsPkXs9ArMQzoBLEDiKRN/view

For additional reporting information, please visit the Colorado Department of Public Health & Environment's website: www.colorado.gov/cdphe/report-a-disease

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

PHI Uses and Disclosures Policy
Attachment 8

Scope of Policy

This policy governs the permitted uses and disclosures of *protected health information (PHI)* for UCCS *designated healthcare components*. All *workforce members* of UCCS *designated healthcare components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated healthcare components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

1. It is the policy of UCCS and its *designated healthcare components* to conduct its operations in full compliance with HIPAA rules governing uses and disclosures of *PHI.*
2. UCCS *designated healthcare components* will apply the *Minimum Necessary Standard* for access and disclosures of *PHI*.
3. UCCS *designated healthcare components* will process requests for information from individual's records in a timely, consistent manner as set forth in this policy.
4. This policy applies equally to all records, including electronic records. No employee shall release any type of records without complying with this policy.

Procedures

1. Permitted or Required Uses or Disclosures.
   A. *PHI* shall not be used or disclosed except in the following circumstances:
      1. The individual who is the subject of the *PHI* requests the individual's own information;
      2. For treatment, payment, or *health care operations*;
      3. For the treatment activities of a health care provider (other than the UCCS *designated healthcare components*);
      4. To another HIPAA *covered entity* or health care provider (other than the UCCS *designated healthcare components*) for the payment activities of the *covered entity* or other health care provider;
      5. To another *covered entity* or health care provider for its *health care operations* so long as the *covered entity* or other health care provider each have or had a relationship with the individual whose *PHI* is being used or disclosed to the *covered entity* or other health care provider and the information pertains to that relationship;
      6. *Incidental disclosures* that are incident to a use or disclosure otherwise permitted or required by this policy and provided that the UCCS *workforce member* or student has applied appropriate safeguards, used the *Minimum Necessary Standard*, and adequately demonstrated that there was no other option;

7. Pursuant to a valid authorization form (Authorization to Release and/or Obtain Patient Information form*)* and in accordance University and UCCS policies that relate to authorization; and
8. As permitted by other applicable policies, including de-identified information, *limited data sets*, and other categories covered under this policy.

B. UCCS *designated healthcare components* will disclose *PHI* to individuals in accordance with Attachment 7 Patient Rights Policy*.*

C. Prohibition of Redisclosure. Unless a law or regulation requires a more specific prohibition on redisclosure (usually for AIDS/HIV, alcohol and drug abuse, and other particularly sensitive medical information), each disclosure outside the UCCS *designated healthcare component* shall contain the following notice:
   1. *The attached medical information pertaining to [Name of client/patient] is confidential and legally privileged. Clinic Name, a UCCS Designated Healthcare Component, has provided it to [Name of recipient] as authorized by the patient. The recipient may not further disclose the information without the express consent of the patient or as authorized by law.*

D. Courtesy Notifications to Provider. As a courtesy, UCCS *designated healthcare component* records processing personnel shall notify the appropriate UCCS *designated healthcare component* healthcare provider when any of the following occur:
   1. Individual or representative requests information from the medical record.
   2. Individual or representative requests direct access to the complete medical record.
   3. Individual or representative institutes legal action.

2. Disclosure Monitoring and Logging.

A. Each UCCS *designated healthcare component* shall maintain a log to track the step-by-step process towards completion of each request for the release of *PHI* (for example, PHI Disclosure Accounting Log). Each director/designate of the UCCS *designated healthcare components* will review and update this log daily to give proper priority to requests and to provide early intervention in problem situations. The log shall contain the following information:
   1. Date department received the request.
   2. Name of patient.
   3. Name and status (patient, parent, guardian) of person making request.
   4. Information released.
   5. Date released.
   6. Fee charged.

B. Disclosure Quality Control. Each UCCS *designated healthcare component* and/or the UCCS *privacy officer* shall conduct a routine audit of the release of information at least annually, paying particular attention to the following:
   1. Validity of authorizations.
   2. Appropriateness of information abstracted in response to the request.
   3. Retention of authorization, request, and transmitting cover letter.
   4. Procedures for telephone, electronic, and in-person requests.
   5. Compliance with designated priorities and timeframes.
   6. Proper processing of fees.

C. Documentation of the Release. Unless the request specifies release of the complete medical record, the UCCS *designated healthcare component* shall release only selected portions of the record.

D. Retention of Disclosure Requests. The UCCS *designated healthcare component* will retain the original request, the authorization for release of information, and a copy of the cover

letter in the individual's medical record for the appropriate record retention period pursuant to Attachment 2 Documentation Policy (Retention).

3. Timeline and Fee Schedule.
   A. Each UCCS *designated healthcare component* will process requests for information from individual's medical records within thirty (30) calendar days and in a consistent manner as set forth in this policy.
   B. Each UCCS *designated healthcare component* will charge a reasonable fee to offset the costs associated with specific categories of requests. Fees shall be based on an assessment of such factors as the costs of equipment and supplies, employee costs, and administrative overhead and shall include postage (including express mail or courier costs) when incurred at the request of the authorizing party. For requests for records in electronic format, HIPAA permits fees to include only direct labor costs when responding to such requests. Individual states have also established maximum fees for copies of patient records.
4. Use of Copying Services. To facilitate the timely processing of release of information requests, UCCS *designated healthcare components* may use the services of a commercial copying service on terms that protect the integrity and confidentiality of patient information.
5. Marking and Fundraising.
   A. Marketing. *PHI* may not be used or disclosed for marketing purposes without a valid authorization, HIPAA Authorization for Release of Health Information – Media form, except in the following circumstances:
      1. If the communication is a face-to-face communication between an employee of a UCCS *designated healthcare component* and the individual; or
      2. If the communication involves only a promotional gift of nominal value provided by the UCCS *designated healthcare component*.
      3. If the marketing involves direct or indirect remuneration to the UCCS *designated healthcare component* from a third party, the authorization must state that remuneration is involved. The UCCS *designated healthcare component* cannot sell *PHI* to any other person or entity.
   B. Fundraising. All fundraising communications must contain a clear and conspicuous opportunity to elect not to receive any further fundraising communications. The method for opting out must not cause the individual to incur an undue burden or more than a nominal cost. Fundraising communications may not be made to an individual who has elected not to receive such communications.
      1. UCCS *designated healthcare components* may use the following *PHI* without a patient's authorization for fundraising purposes:
         i. Patient demographic data (name, address, phone/email, date of birth, age, gender, etc.);
         ii. Health insurance status;
         iii. Dates of patient services;
         iv. General type of department in which a patient is serviced;
         v. Treating physician information; and
         vi. Outcome information.
      2. *PHI* requiring written patient authorization prior to fundraising use includes:
         i. Diagnosis;
         ii. Nature of services; and
         iii. Treatment.
6. De-Identification of Data. There are two methods of de-identification: 1) use of statistical methods proven to render information not individually identifiable, and 2) deletion of 18 specified identifiers. Once *PHI* has been de-identified, it is no longer *PHI*, and the restrictions

and requirements of federal and state privacy laws no longer apply. However, if a re-identification code is added to the data, certain privacy and security rules apply to the code. Specific questions regarding this should be addressed to the UCCS *privacy officer* and/or the UCCS *security officer*.

7. Training Requirements. Each UCCS *designated healthcare component* shall give periodic in-service training to all employees involved in the release of information.
8. Authorization.
   A. All disclosures must have a written, signed, current, valid authorization to release medical information as follows:

Patient Category	Required Signature
Adult Patient	The patient or a duly authorized representative, such as court-appointed guardian or attorney. Proof of authorized representation required (such as notarized power of attorney).
Deceased Patient	Next of kin as stated on admission face sheet (state relationship on authorization) or executor/ administrator of estate.
Unemancipated Minor	Parent, next of kin, or legally appointed guardian or attorney (proof of relationship required).
Emancipated Minor	Same as adult patients above.
Psychiatric, drug, alcohol program patients/clients	Same as adult patients above, but check for special requirements
AIDS/HIV or other sexually transmitted disease patients	Same as adult patients above, but check for special requirements

   B. Forms. Each UCCS *designated healthcare component* shall use the Authorization to Release and/or Obtain Patient Information form whenever possible. Each UCCS *designated healthcare component* shall, however, honor letters and other forms, provided the letter or form includes all the required information. Specific questions regarding whether a third party's letter or form is sufficient can be directed to the UCCS *privacy officer* and/or legal counsel.
   C. Revocation. An individual may revoke an authorization by submitting the Revocation of Authorization form to the appropriate UCCS *designated healthcare component*. The revocation shall become effective when the UCCS *designated healthcare component* receives it but shall not apply to disclosures already made.
   D. Refusal to Honor Authorization. UCCS *designated healthcare components* and/or the UCCS *privacy officer* and/or others authorized to release information will not honor an individual's authorization when there is reasonable doubt or question as to the following information:
      1. Identity of the person presenting the authorization. For process of verification, each UCCS *designated healthcare component* shall use the table below.

2. Status of the individual as the duly appointed representative of a minor, deceased, or incompetent person.
3. Legal age of or status as an emancipated minor.
4. Patient capacity to understand the meaning of the authorization.
5. Authenticity of the patient's signature.
6. Current validity of the authorization.
7. In such situations, the UCCS *designated healthcare component* shall refer the matter to the UCCS *privacy officer* for review and decision.

Person and Identity Verification Table

Person to Identify	**In-Person Encounter**	**Telephone Encounter**	**Request in Writing** (Fax, mail, hand-delivered)
Attorney	▪ Presents with business card and photo identification (i.e. driver's license or organization ID badge)	▪ It would be difficult to verify identity and authority by phone. Verification in person or in writing may be required	▪ Supplies business card, photo identification (i.e. driver's license or org ID badge), letterhead. Confirmation call is required.
Patient	▪ Patient provides name, address, and date of birth and/or social security number; or ▪ Acquainted with patient	▪ Patient provides name, address, and date of birth and/or social security number; or ▪ Acquainted with patient	▪ Patient provides name, address, and date of birth and/or social security number. Verify patient's signature with that on file or on driver's license.
Personal Representative (Legal Guardian) for the Patient	▪ Personal Rep provides patient's name, address, and date of birth and/or social security number, **and** verifies (via legal docs) relationship to patient; or, ▪ Acquainted with personal Rep	▪ Personal Rep provides patient's name, address, and date of birth and/or social security number, **and** verifies (via legal docs) relationship to patient; or, ▪ Acquainted with Personal Rep as such.	▪ Personal Rep provides patient's name, address, and date of birth and/or social security number. Verify the Personal Rep's signature with signature on file or on driver's license.
Persons Involved in the Patient's Immediate Care *(PHI relevant only*	▪ Patient actively involves this person in his/her care; or	▪ Patient actively involves this person in his/her care; or	▪ N/A

Person to Identify	In-Person Encounter	Telephone Encounter	Request in Writing (Fax, mail, hand-delivered)
to the patient's current care (164.510(b)). ▪ Blood Relative ▪ Spouse ▪ Domestic Partner ▪ Roommate ▪ Boy/Girl Friend ▪ Neighbor ▪ Colleague	▪ In your best professional judgment, the disclosure is in the patient's best interest.	▪ In your best professional judgment, the disclosure is in the patient's best interest. ▪ Use call-back.	
Power of Attorney (POA) for the Patient	▪ Presents with a photo ID and a copy of the POA. Verify patient's signature with one on file. ▪ Acquainted with power of attorney	▪ Previously obtained a copy of the POA and verified the patient's signature with one on file. ▪ Acquainted with power of attorney as being such	▪ Obtain a copy of the POA and verify the patient's signature with one on file
Provider from Another Facility	▪ Acquainted with provider as a treatment provider; ▪ Provider is wearing a photo badge from his/her facility; or, ▪ Patient/personal representative introduces provider to you.	▪ Acquainted with provider as a treatment provider; or; ▪ Call requestor back through main switchboard number (not via a direct number).	▪ Recognize name of facility and address on letterhead as a treatment facility; or ▪ Call requestor back through main switchboard number (not via a direct number).
Public Official ▪ CIA ▪ Court Order ▪ FBI ▪ Law Enforcement Officer ▪ OCR ▪ OIG ▪ Public Health Agency Official ▪ Other	▪ Presents an agency I.D. badge; ▪ Presents with a written statement of legal authority; ▪ Presents with a written statement of appointment on appropriate government letterhead; ▪ Presents with warrant, court order, or legal process issued by a grand jury, or a	▪ Official states release is necessary to prevent or lessen the threat to the health/safety of a person/public.	▪ Written statement of legal authority; ▪ Written statement of appointment on appropriate government; ▪ Warrant, court order, or other legal process issued by a grand jury or a judicial or administrative tribunal; or ▪ Contract for services or purchase order

Person to Identify	In-Person Encounter	Telephone Encounter	Request in Writing (Fax, mail, hand-delivered)
	judicial or admin. tribunal; ▪ Presents with a contract for services or purchase order; or, ▪ Official states release is necessary to prevent or lessen the threat to the health/safety of a person/public.		
Vendor Who Assists with Treatment, Payment, or Health Care Operations Examples Include, But Are Not Limited to the Following: ▪ Accreditation Org. ▪ DME Company ▪ Insurance Co. ▪ Pharmacy Vendor We Have Rebate Agreement with ▪ Software Vendor ▪ Statement Vendor	▪ Recognize requestor/ organization; or ▪ Photo identification with organization	▪ Recognize requestor or organization	▪ Recognize requestor/ organization; or ▪ Call requestor back through main switchboard number (not via a direct number).
***Workforce Member* of Our Organization**	▪ Acquainted with individual as a *workforce member*; or, ▪ *Workforce member* is wearing an I.D. badge.	▪ Acquainted with individual as a *workforce member*; or, ▪ *Workforce member* is calling from an in-house extension.	▪ Request is sent from/through our own computer system; or ▪ Request is on our own letterhead.
Non-*Workforce Member* of Our Organization	▪ No access granted unless approved by legal and compliance	▪ No access granted unless approved by legal and compliance	▪ No access granted unless approved by legal and compliance

PHI Disclosures Table

Disclosures should follow Attachment 7 Patient Rights Policy, what is included in a *designated record set*

Requestor	Authorization Required?	Copy Fee Charged?	Track on Disclosure Accounting?
Accrediting Agencies (JCAHO, CARF)	No	No	No
Attorney for Facility/Corporation	No	No	No
Contractors/*Business Associates*	No, unless their purpose falls outside of TPO.	No	No
For Deceased Persons ▪ Coroner or Medical Examiner, Funeral Directors ▪ Organ Procurement	No	No	Yes
Employer ▪ *PHI* specific to work related illness or injury, and ▪ Required for employer's compliance with occupational safety and health laws	No, for the purpose listed. Yes, for all others.	No	No
Family Members	No for oral disclosures to family members involved in care so long as patient consents (orally or in writing); Yes, for others.	Yes	No
Entity Subject to the Food and Drug Administration ▪ Adverse events, product defects or biological product deviations ▪ Track products ▪ Enable product recalls, repairs, or replacements ▪ Conduct post marketing surveillance	No	No	Yes
Health Oversight ▪ Government benefits program ▪ Fraud and abuse compliance ▪ Civil rights laws ▪ Trauma/tumor registries ▪ Vital statistics ▪ Reporting of abuse or neglect	No	No	Yes
Health Care Practitioners and Providers for Continuity of Treatment and Payment	No	No	No

Requestor	Authorization Required?	Copy Fee Charged?	Track on Disclosure Accounting?
Health Care Practitioners and Providers if <u>not</u> Involved in Care or Treatment (i.e., consultants)	No	No	No
Insurance Companies/Third Party Payors ▪ Related to Claims Processing	No	No	No
Judicial and Administrative Proceedings ▪ Court order, or warrant ▪ Subpoena	No No - See Subpoena Policy	No Yes	Yes Yes
Law Enforcement ▪ Administrative request ▪ Locating a suspect, fugitive, material witness or missing person ▪ Victims of crime ▪ Crimes on premises ▪ Suspicious deaths ▪ Avert a serious threat to health or safety	No	No	Yes, except for disclosures to correctional institutions.
Public Health Authorities ▪ Surveillance ▪ Investigations ▪ Interventions ▪ Foreign governments collaborating with US public health authorities ▪ Recording births/deaths ▪ Child/elder abuse ▪ Prevent serious harm ▪ Communicable disease	No	No	Yes
Research (w/o Authorization) (See Attachment 9 Uses and Disclosures for Research Purpose)	No, if IRB or *Privacy Board* approves research study and waives authorization.	No	Yes
Specialized Government Functions ▪ Military and Veterans' activities ▪ Protective services for the President ▪ Foreign military personnel ▪ National security and intelligence activities	No	No	Yes, except for disclosures for national security and intelligence activities.

Requestor	Authorization Required?	Copy Fee Charged?	Track on Disclosure Accounting?
Workers' Compensation ▪ Comply w/existing laws (see state law)	No	See applicable State Law	Yes

Related Policies

APS 2027 Code of Conduct
APS 6002 Electronic Communications
APS 6005 IT Security Program
APS 6010 Data Governance
Reporting and filing a complaint (see Compliance and Ethics Website)
UCCS Policy 700-001 Email as Official Means of Communication
UCCS Policy 800-002 Social Media Policy

Reference

45 CFR § 164.502 to 164.514
6 Colo. Code Regs. § 1011-1:IV-8.102
C.R.S. § 25-1-801
6 Colo. Code Regs. § 1011-1:II-5.2
Colo. Code Regs. §§ 502-1:21.170.2; 502-1:21.170.3

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

Use and Disclosure for Research Purposes
Attachment 9

Scope of Policy

This policy governs the privacy circumstances under which *protected health information (PHI)* may be disclosed for *research* purposes for UCCS and its *designated healthcare components*. All *workforce members* of UCCS *designated healthcare components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated healthcare components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

1. It is the Policy of UCCS and its *designated healthcare components* to permit use and disclosure of the *PHI* it maintains for *research* only as provided in this policy, regardless of the source of funding of the *research*. Specifically, UCCS *designated healthcare components* will only permit *research* use and disclosure of the *PHI* as follows:
   A. When the individual who is the subject of the *PHI* provides prior authorization (Authorization to Use or Disclose Identifiable Health Information for Research form);or
   B. Without the individual's prior authorization if:
      1. Documentation (Activities Preparatory to Research Request for Waiver form) submitted to the *privacy board* for approval is obtained from the researcher that the use or disclosure of the *PHI* is solely for preparation for *research*, e.g., to prepare a *research* protocol or check subject eligibility;
      2. The researcher submits adequate documentation (Required Representations for Research on Decedents Information form) to the *privacy board* for approval that the use or disclosure of the *PHI* is solely for *research* on decedents;
      3. The *privacy board* has approved a waiver or alteration of the authorization requirement (Request for Waiver of Elements of Authorization or an Altered Authorization form*);*
      4. The *PHI* is de-identified in compliance with HIPAA's *limited data set* or de-identification requirements;
      5. *Research* qualifies for the transition provisions because it was obtained prior to the date of 4.15.03. (45 CFR 164. 532 (a) and (c)).

Procedures

1. Accounting for Disclosures. Participating in *research* does not change the subject's rights to the accounting of disclosure. Each UCCS *designated healthcare component* must develop a policy and/or procedure related to how the *designated healthcare component* will provide an accounting as per Attachment 7 Patient Rights Policy.
2. *Privacy Board* Procedures and Forms. *Privacy Board* Standard Operating Procedures (SOP) and forms are located on the Compliance website under the *Privacy Board* category

https://www.uccs.edu/compliance/news/privacy-board. The *Privacy Board* SOP covers procedures related to Section B above.

3. Use and Disclosures of *PHI* for *Research* with Authorization
   A. Notice of Privacy. It is required that all individuals entering a research protocol be given the UCCS Notice of Privacy Practices. The Notice of Privacy Practices is often given to a *research* subject upon registration. If a *research* subject does not enter the *research* setting through clinic registration, then the *research* team is responsible for providing the notice to subjects. A copy of the signature page acknowledging receipt of the notice should be kept in the subject's *research* file.
   B. Obtain Authorization. The members of the *research* team must determine that it is necessary (or mandated, in the case of clinical research trials) to obtain the individual's authorization. They will ensure that the Authorization to Use or Disclose Identifiable Health Information for Research form discloses how the individual's *PHI* will be used or disclosed and contains the following:
      1. Description of the *PHI* to be used or disclosed, and must describe identifying information in a specific and meaningful manner;
      2. Names and specific identification of persons (all classes of persons) authorized to request, use or disclose the information required;
      3. Names and specific identification of persons (all classes of persons) or institutions receiving the *PHI* disclosure (example: data coordinating centers, sponsors, IRB's, Data Safety Monitoring Boards);
      4. A description of each purpose for use or disclosure;
      5. Expiration date or event that relates to the purpose of the disclosure (example: "end of research" or "no expiration");
      6. A statement that the subject has the right to revoke the Authorization, a description of the revocation process, and a list of all exceptions;
      7. Whether treatment, payment, enrollment, or eligibility can be conditioned on the authorization (including research-related treatment) and consequences of refusing to sign the authorization (Example: "*research* may not be allowed to continue if authorization is withheld." Refer to Section 3.E. Refusal to Sign Authorization or Revoking Authorization);
      8. A statement of the potential risk that the *PHI* will be re-disclosed by the researcher or any other recipient. This may be a general statement that the HIPAA Privacy Rule may no longer protect *health information* disclosed to the recipient;
      9. Statement that the authorization is for a specific research protocol and that authorizations for future unspecified *research* are not permitted; and
      10. Subject signature and date.
   C. Legal Representative. If the authorization is to be signed by someone other than the *research* subject, the members of the *research* team will ensure that the person signing has appropriate authority as the individual's personal representative as set forth in Attachment 8 PHI Uses & Disclosures Policy.
   D. Access to *Research* Records in Blinded Clinical Trials. Patients have the right to access, inspect, and obtain copies of their *research* records. However, the access provisions do not require that individuals be provided with access to their *PHI* the entire time they are participating in a clinical trial, so long as the Authorization adequately informs them of their rights. For blind clinical trials, the authorization form must state that individuals will not be provided access to their *PHI* while the clinical trial is open. By limiting the individual's access to their *PHI* through the duration of the clinical trial, the "blinding" aspects of the *research* and the design of the *research* protocol are preserved. This limited access does not affect

research subjects' legal rights and should be necessary only during the treatment phase of the *research*/clinical trial.

E. Refusal to Sign Authorization or Revoking Authorization. In the event an individual refusesto sign an authorization or revokes a current authorization, the members of the *research* team may consult with the Institutional Review Board (IRB) chair (or designee) and/or *Privacy Board* chair to determine if the individual should be denied enrollment in the trial. The members of the *research* team shall be responsible for documenting any decision to deny participation in the trial and providing the individual with a written statement of such a decision. A copy of the written letter must be placed in the *research* file.

F. Amendment of Authorization. If the individual's authorization is obtained, the individual's *PHI* can be used and disclosed in the manner that is consistent with the terms of the authorization. If any person wishes to use or disclose the *PHI* for a purpose that is not set forth in the original authorization, the members of the *research* team are responsible for ensuring that a second authorization is obtained prior to such use or disclosure.

4. Coded Information. Researchers using a *limited data set* may utilize unique codes or identifiers. The code may not replicate a part of a listed direct identifier. For example, the code or *limited data set* cannot include the last four digits of a social security number or ID number. Use of statistical methods to render a code is permitted so long as the code is not individually identifiable, and risk of re-identification is very small.
5. Specimen Repositories. Identifiable specimens should be coded or de-identified to provide adequate protection. All protections and procedures listed in this Policy apply to the use of identifiable *research* specimens.
6. Electronic and Internet *Research*. All users of *research* data utilizing remote access are responsible for ensuring that their use of computers (internal and external), networks, and the Internet will not compromise the security of the *PHI* or technology resources. No *PHI* may be removed from a UCCS *designated health care component* without permission. Access to the *PHI* through a remote access connection is not itself a removal of the *PHI*, but the printing, copying, saving or faxing of the *PHI* is considered a removal. *Research* that involves web access must have proper data security measures in place. Questions about specific security measures may be directed to the UCCS *security officer*.
7. Disclosures Required by Law: UCCS *designated health care components* may be required by law to use or disclose *PHI* in the following circumstances:
   A. To cancer registries;
   B. Disclosure to the federal government of data first produced under a federal award;
   C. Activities for purposes of preventing or controlling disease, injury or disability (for example, reporting to the National Institute of Health, Food and Drug Administration or Centers for Disease Control, Department of Health and Human Services or Morbidity and Mortality Weekly Report);
   D. Reporting to Office of Sponsored Programs and Research Integrity for compliance of *research* activity.

Related Policies

APS 2027 Code of Conduct
Office of Sponsored Programs Website
Privacy Board Standard Operating Procedures
Reporting and filing a complaint (see Compliance and Ethics Website)
Research Misconduct Procedures & Guidelines

Reference

45 CFR § 164.508
45 CFR § 164.512 (i)
45 CFR § 164.514 (e)

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

Privacy Complaints Policy
Attachment 10

Scope of Policy

This policy governs the privacy complaints process for UCCS and its *designated health care components*. All *workforce members* of UCCS *designated health care components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated health care components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

1. It is the Policy of UCCS and its *designated health care components* to respond in a timely and positive manner to all complaints submitted by any persons or parties, including patients, *workforce members*, and any other person or party.
2. UCCS and its *designated health care components* must comply with HIPAA and the HIPAA implementing regulations pertaining to privacy complaints in accordance with the requirements at § 164.530(a) and § 164.530(d), as amended by the HITECH Act of 2009 (ARRA Title XIII), and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013).
3. HIPAA regulations, at § 164.530(g), prohibit intimidating or retaliatory acts against any person or patient who files a privacy complaint or exercises any Right guaranteed under HIPAA.
4. Responsibility for the acceptance of, management of, and responses to privacy complaints shall reside with the UCCS *privacy officer*, who shall establish a process and appropriate forms to receive and process complaints.

Procedures

1. Complaints can be submitted anonymously through a third party vendor, EthicsPoint, at https://secure.ethicspoint.com/domain/media/en/gui/14973/index.html.
2. Complaints can be submitted in written form (Privacy Complaint Form), dated and signed by the complainant. The University will treat complaints received through other means, like email, telephone, or in-person conversation, in a similar manner.
3. The UCCS *privacy officer*, in conjunction with the UCCS *designated health care component's* director/designate, shall investigate and respond to all written complaints with a written response within 30 days of the time each complaint is received. If more time is required to investigate and resolve a specific complaint, the complainant shall be notified in writing, within 30 days of the time each complaint is received, that additional time is required to investigate and resolve the complaint. In no case shall more than 60 days elapse between the time a complaint is received and the resolution of the complaint.

4. The UCCS *privacy officer* shall investigate each and every complaint in a fair, impartial, and unbiased manner. All parties named in the complaint, or who participated in events leading to the complaint, shall be interviewed in a non-threatening and non-coercive manner.
5. The final resolution or disposition of each written complaint shall be documented, and a summary of the findings shall be provided to the complainant within 30 days of the time each complaint is submitted in writing, unless the additional 30 days of response time is invoked, as above. The final resolution or disposition shall be retained in accordance with Attachment2 Documentation Policy (Retention).
6. In addition to providing complainants with a written response to their complaint, complaints that are found to have merit will be resolved with some remediation that is appropriate to the severity of the situation. Such remediations may include, but are not limited to:
   A. A written apology to the complainant from our organization.
   B. Credit-monitoring service for the complainant for a period of one or two years, paid for by our organization, when the complaint involves a breach of unsecured individually identifiable *health information* that has been compromised or put at risk by our actions.
   C. Financial compensation, if determined to be appropriate by legal counsel and senior management.
   D. Sanctions against *workforce members*, as appropriate to the circumstances.
   E. Other unspecified remediation(s), as determined by legal counsel and senior management.
7. For complaints submitted to the federal government, it is the Policy of UCCS and its *designated health care components* to cooperate fully and openly with federal authorities as they conduct their investigation, as specified in Attachment 4 HIPAA Investigations Policy.
8. No officer, agent, employee, contractor, temporary worker, student, or volunteer of UCCS and its *designated health care components* shall obstruct or impede any investigation in any way, whether internal or federal.

Related Policies

APS 2027 Code of Conduct
Reporting and filing a complaint (see Compliance and Ethics Website)

Reference

45 CFR § 164.530(a)
45 CFR § 164.530(d)

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

Risk Management and Risk Analysis Policy
Attachment 11

Scope of Policy

This policy governs risk analysis for UCCS *designated health care components*. All *workforce members* of UCCS *designated health care components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated health care components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

1. It is the responsibility of anyone at UCCS who uses, discloses or maintains *protected health information (PHI)* to practice security management. This includes faculty, staff, students, trainees, volunteers, etc. The UCCS *security officer* is responsible for overall periodic campus risk analyses, compliance program evaluations, and maintenance.
2. It is the Policy of UCCS and its *designated health care components* to establish, implement, and maintain an appropriate risk management process.
3. Business and information-technology "best practices", along with the research and recommendations of the National Institute for Standards and Technology (NIST), shall be included in the development and execution of the risk management process
4. Such a risk management process shall be under the direct control and supervision of the designated UCCS *privacy officer* and UCCS *security officer*, and shall involve legal counsel, the UCCS Office of Information Technology (OIT), UCCS *designated health care component* leadership, and any other parties or persons deemed to be appropriate.
5. This process shall strive to identify, analyze, prioritize, and minimize identified risks to information privacy, security, integrity, and availability. The nature and severity of various risk and risk elements shall be identified and quantified, with the goal of reducing risk as much as is practicable. The risk management process shall be ongoing, and shall be updated, analyzed, and improved on a continuous basis.
6. Risk management results shall be used for management's decision-making processes, in order to help reduce our overall risk and to comply with HIPAA and other applicable laws and regulations.

Procedures

1. Security Management Process. All members of the UCCS workforce who create, receive, maintain or transmit *PHI* must implement policies and procedures to prevent, detect, contain, and correct security violations.
2. Risk Analysis

A. It is the responsibility of each UCCS *designated health care component's* leadership in conjunction with the UCCS *privacy officer* and the UCCS *security officer* to conduct risk assessments to understand and document risks from security failures that may cause loss of confidentiality, integrity, or availability. Risk assessments should take into account the potential adverse impact on the University's reputation, operations, and assets. The risk assessment will be completed and documented using the HIPAA Walkthrough Checklist and the HIPAA Security Workbook ("Workbook").

B. It is the responsibility of the UCCS *privacy officer* and the UCCS *security officer* to conduct HIPAA walkthroughs of each UCCS *designated health care component* at least every two years.

C. It is the responsibility of the UCCS *security officer* and the director/designate of each UCCS *designated health care component* to complete the Workbook pursuant to this procedure. The completed Workbook will be approved by the UCCS *security officer* and treated as documentation of HIPAA procedures. The completed Workbook should be used by each UCCS *designated health care component* for policy implementation, enforcement, and training. A copy of completed Workbooks must be kept on file and easily accessible to the workforce by each UCCS *designated health care component* and the UCCS *privacy officer* and the UCCS *security officer*.

1. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to identify relevant information systems and electronic information resources that require protection.
2. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to review and update risk assessments annually, or more frequently in response to significant legislative, environmental, or operational changes.
3. It is the responsibility of the director/designate of each UCCS *designated health care component* to inform the UCCS *privacy officer* and UCCS *security officer* of the completion of all documented risk assessments withinthirty (30) calendar days of their completion and provide a copy upon request.

3. Risk Management

A. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *privacy officer* and the UCCS *security officer* to select appropriate controls, e.g. policies, procedures, technologies, to safeguard data relative to the sensitivity or criticality determined by the risk assessment and to document the individual(s) responsible for implementation of each recommendedpractice.

B. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to, where possible, incorporate these standards and practices when evaluating and selecting new hardware and software.

Related Policies

APS 2027 Code of Conduct
APS 6002 Electronic Communications
APS 6005 IT Security Program
APS 6010 Data Governance
Reporting and filing a complaint (see Compliance and Ethics Website)
UCCS Policy 700-001 Email as Official Means of Communication
UCCS Policy 800-002 Social Media Policy

Reference

164.302 to 164.318

164.308(a)(1)
The Health Information Technology for Economic and Clinical Health Act (HITECH Act)
National Institute for Standards and Technology ("NIST")

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

Sanction Policy
Attachment 12

Scope of Policy

This policy governs workforce sanctions and disciplinary actions for UCCS and its *designated health care components*. All *workforce members* of UCCS *designated health care components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated health care components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

1. It is the Policy of UCCS and its *designated health care components* to establish and implement appropriate, fair and consistent sanctions for *workforce members* who fail to follow established policies and procedures, or who commit various offenses.
2. Sanctions will be imposed pursuant to applicable HIPAA policies.
3. Offenses involving obvious illegal activity related to patient privacy may result in notifications to appropriate law enforcement authorities.
4. It is the Policy of UCCS and its *designated health care components* to fully document all workforce sanctions and their dispositions, according to our Documentation Policy and HIPAA requirements.

Procedures

1. The UCCS *privacy officer* and UCCS *security officer* will investigate all alleged violations of UCCS HIPAA policies, and will document the allegations and their eventual resolution, including any disciplinary actions taken. The UCCS *privacy officer* will maintain all official documentation related to privacy violations. The UCCS *security officer* will maintain all official documentation related to security violations.
2. All affected departments and/or individuals shall cooperate fully with the investigation. The UCCS *privacy officer* and the UCCS *security officer* shall keep UCCS administration apprised of ongoing investigations as appropriate. Given the nature of some of these investigations, there are times when the scope of the problem must be determined before notification is possible.
3. The determination of what, if any, disciplinary action will be taken will be made in accordance the applicable disciplinary procedures. The UCCS *privacy officer* and/or the UCCS *security officer* will assist the disciplinary authority in determining an appropriate disciplinary action that is based on the relative severity of the violation.

Related Policies

APS 2027 Code of Conduct

Reporting and filing a complaint (see Compliance and Ethics Website)

Reference

45 CFR § 164.308(a)(1)

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

Information System Activity Review/ Authorization and Supervision Policy/Log-in Monitoring Policy Attachment 13

Scope of Policy

This policy governs information systems activity reviews for UCCS *designated health care components.* All *workforce members* of UCCS *designated health care components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated health care components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

1. It is the Policy of UCCS and its *designated health care components* to only permit *workforce members* who have been appropriately authorized to have access to individually identifiable *health information*.
2. It is the Policy of UCCS and its *designated health care components* to properly supervise *workforce members* who have access to individually identifiable *health information*.
3. Proper authorization to access individually identifiable *health information*, and appropriate supervision of *workforce members* authorized to access individually identifiable *health information* can help reduce our overall risk and reduce the likelihood of data breaches and HIPAA violations.
4. *Workforce members* shall have access only to the individually identifiable *health information* that they need in order to perform their work-related duties.
5. It is the Policy of UCCS and its *designated health care components* to document the authorization and supervision of all *workforce members* who have access toindividually identifiable *health information*.
6. Regular monitoring of log-ins and log-in attempts is a proven approach to controlling access to sensitive information systems and data, and to detecting inappropriate information systems activity.
7. Discrepancies and potentially inappropriate or illegal activities shall immediately be brought to the attention of the UCCS *privacy officer*, the director/designate of the UCCS *designated health care component*, legal counsel, and/or Human Resources, as appropriate.
8. UCCS shall assess potential risks and vulnerabilities by both reviewing information system activity, as well as developing, implementing, and maintaining appropriate administrative, physical, and technical security measures in order to detect and minimize security violations involving *protected health information (PHI)*. These protective measures give UCCS the ability to identify unauthorized data access activities, assess security safeguards, and respond to potential weaknesses.

9. It is the Policy of UCCS and its *designated health care components* to regularly review various indicators and records of information system activity, including, but not limited to: audit logs, access reports, and security incident reports.
10. The goal of this policy is to prevent, detect, contain, and correct security violations and threats to individually identifiable *health information*, whether in electronic or any other forms.
11. It is the policy of UCCS and its *designated health care components* to document all information system activity review activities and efforts.

Procedures

1. General.
   A. Each UCCS *designated health care component* director/designate shall determine which individuals are authorized to work with *PHI* in accordance with a role-based approach.
   B. It is the responsibility of the director/designate of each UCCS *designated health care component* to authorize and supervise *workforce members*' access to individually identifiable *health information*.
   C. Any violations discovered during review will be reported to the UCCS *privacy officer* or UCCS *security officer* as outlined on the UCCS Office of Information Technology (OIT) website under "Incident Response" https://www.uccs.edu/it/security/incident-response.html.
   D. UCCS OIT maintains an internal security control program. Procedures, policies, and record-keeping activities have been established to ensure proper legal and ethical business practices. This program complements the user authentication process and may act as a deterrent to internal abuse by making users aware that audit trails, file access reports, and security incident tracking reports are produced, reviewed and investigated. Violations are subject to applicable sanctions. The internal security control program may take various forms including regular information system activity review. These reviews incorporate login monitoring, automated reports of audit trails or logs, file access reports, and manually produced security incident trackingreports.
2. Audit Controls. UCCS OIT will monitor audit records from firewall and other network protection layer logs, domain logs including login and data access activity, and event logs from host operating systems.
   A. Audit Control and Review Plan. An audit control and review plan must be developed by each UCCS *designated health care component's* director/designate that hosts *PHI* and must be approved by the UCCS *security officer*. If the UCCS *designated health care component's PHI* inventory changes, causing its audit control and review plan to change, the plan must be re-evaluated and re-submitted to the UCCS *security officer*. The plan must include:
      1. Systems and applications to be logged;
      2. Information to be logged for eachsystem;
      3. Login reports for each system; and,
      4. Procedures to review all audit logs and activity reports, including identifying each *workforce member* responsible for performing the audit, the frequency the audit is to be performed, and escalation procedures if suspicious activity is detected.
   B. Audit Trail. The audit trail provides a means to monitor user activity and detect suspicious activity and/or breaches. It also provides the ability to reconstruct events where data integrity may be questioned and functions as a deterrent to misuse by *workforce members*. The audit trail process includes the implementation of hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use *PHI*.
      C. Audit Trail Mechanisms.

1. The mechanisms used to capture audit trail information may include use of automated tools designed to report suspicious activity or use of automated warning messages that appear prior to access of sensitive information. System hardware, software, and applications must have the capability of creating log files. These logs must include, but are not limited to:
    a. user ID;
    b. login date/time; and,
    c. activity time.
2. Audit logs may include system and application log-in reports, activity reports, exception reports or other mechanisms to document and manage system and application activity. Audit control mechanisms for systems containing low risk *PHI* (determined duringthe regular risk assessment) are not required.

D. Workforce Accountability. The director/designate of each UCCS *designated health care component* must educate their *workforce members* on the UCCS *designated health care component's* specific audit procedures and requirements as necessary. This includes incorporating the concept of audit trail and individual user accountability.

3. Information System Activity Review. Each UCCS *designated health care component* that hosts *PHI* must regularly review records of information system activity, such as audit logs, file access reports, and security incident reports. Routine review of information systems activity provides an automatic trail of user actions whenever *PHI* is accessed or modified. This review promotes individual user accountability and gives UCCS the ability to reconstruct significant events or examine suspicious activities as necessary.
    A. Conducting the Review.
        1. Each UCCS *designated health care component* must designate an individual responsible for conducting the review of information systems activity and determine the frequency with which the review will be conducted, based on the UCCS *designated health care component's* audit control and review plan.
        2. To support an effective review, the following information should be examined: audit trails or logs; file access reports; and security incident tracking reports. If suspicious activity is detected, the reviewer should collect: type of event; date and time of occurrence; user ID; and, program used.
    B. Whoever discovers misuse or suspicious activity must contact the director/designate of the UCCS *designated health care component* and the UCCS *security officer*.
4. Log-in Monitoring. As part of the audit control and review plan, each UCCS *designated health care component* must monitor login success and failure to systems that host *PHI*. To ensure that unauthorized login attempts are discovered, whoever discovers discrepancies or unusual login patterns must report such activity to the director/designate of the UCCS *designated health care component* and the UCCS *securityofficer*.
    A. Monitoring of audit trails should be performed with the help of an automated alerting tool or periodic manual review of the logs.
    B. The director/designate of the UCCS *designated health care component* must educate the *workforce members* on the specific procedures and reporting requirements for log-in monitoring.
5. Retention.
    A. Audit trails, file access reports, and automated security incident reports in exact and retrievable copy form must be retained in a secure manner, taking into consideration system capability, space issues, and modality. The method of retention and length of time these reports are to be retained is to be determined by the director/designate of the UCCS *designated health care component* and included in the audit control and review plan.

B. All UCCS *designated health care components'* HIPAA procedures, documentation of decisions made, information system activity reviews, and investigations conducted pursuant to this policy must be retained for a period of no less than six (6) years from the date the policy was last in effect or from the date the decision or investigation was made.

Related Policies

APS 2027 Code of Conduct
APS 6005 IT Security Program
APS 6010 Data Governance
Reporting and filing a complaint (see Compliance and Ethics Website)
UCCS Policy 700-005 Computer Security Incident Response

Reference

45 CFR § 164.302 to 164.318
45 CFR § 164.308
45 CFR § 164.308(a)(3)
The Health Information Technology for Economic and Clinical Health Act (HITECH Act) National Institute for Standards and Technology (NIST)

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

Workforce Clearance and Access/Termination Policy
Attachment 14

Scope of Policy

This policy governs workforce clearance and screening (pre-employment and post-employment) for UCCS *designated health care components*. All *workforce members* of UCCS *designated health care components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated health care components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

1. It is the Policy of UCCS and its *designated health care components* to provide the appropriate level of access to individually identifiable *health information* to all members of the workforce.
2. It is the Policy of UCCS and its *designated health care components* to acknowledge a duty and responsibility to support and facilitate the timely and unimpeded flow of *health information* for lawful and appropriate purposes.
3. The level of access to individually identifiable *health information* for *workforce members* shall be based upon the nature of each *workforce member's* job and its associated duties and responsibilities. *Workforce members* shall have access to all of the individually identifiable *health information* that they need to do their jobs, but no more access than that.
4. No *workforce member* shall have access to a higher level of individually identifiable *health information* than the level for which they have been cleared.
5. Workforce clearance shall specifically incorporate required background screening in accordance with the UCCS Campus Policy 300-022 Employment Background Checks.
6. It is the Policy of UCCS and its *designated health care components* to fully document all workforce clearance-related activities and efforts.

Procedures

1. General.

A. It is the responsibility of the director/designate of each UCCS *designated health care component* to identify a member of the workforce who is responsible for the development and implementation of the policies and procedures required by this procedure.

B. It is the responsibility of the director/designate of each UCCS *designated health care component*, as well as the UCCS *security officer* and the UCCS Office of Information Technology (OIT) to implement policies and procedures to ensure that all workforce members have appropriate access to *electronic protected health information (ePHI)*, as provided below, and to prevent those workforce members who do not have access from obtaining access to *ePHI*.

C. It is the responsibility of the director/designate of each UCCS *designated health care component* as well as the UCCS *security officer* to implement procedures for the authorization and/or supervision of *workforce members* who work with *ePHI* or in locations where it might be accessed.

D. It is the responsibility of the director/designate of each UCCS *designated health care component* to determine which individuals are authorized to work with *ePHI* in accordance with a role-based approach.

2. Workforce Clearance Procedure.
   A. It is the responsibility of the director/designate of each UCCS *designated health care component* as well as the UCCS *security officer* to implement procedures to determine that the access of a *workforce member* to *ePHI* is appropriate.
   B. It is the responsibility of the director/designate of each UCCS *designated health care components* to review role definitions and assignments for appropriateness at least annually.
   C. It is the responsibility of the director/designate of each UCCS *designated health care component* to review access management procedures for appropriateness at least annually.
3. Access Authorization.
   A. It is the responsibility of the director/designate of each UCCS *designated health care component* to implement policies and procedures for granting access to *ePHI*, including through access to a workstation, transaction, program, process, or other mechanism.
   B. It is the responsibility of the director/designate of each UCCS *designated health care component* as well as the UCCS *security officer* to ensure there is a formal system for authorizing user access to *ePHI*, such as an account request form requiring management approval.
   C. It is the responsibility of the director/designate of each UCCS *designated health care component* to ensure access is to be granted in accordance with a role-based approach.
   D. It is the responsibility of the director/designate of each UCCS *designated health care component* to maintain documentation of all authorized users of *ePHI* and their access levels.
   E. It is the responsibility of the director/designate of each UCCS *designated health care component* to ensure *workforce members* must receive security awareness and HIPAA training prior to obtaining access to *ePHI* see Attachment 6 HIPAA Training Policy.
   F. It is the responsibility of the director/designate of each UCCS *designated health care component* as well as the UCCS *security officer* to ensure HIPAA systems must have the capacity to set access controls.
4. Access Establishment and Modification.
   A. It is the responsibility of the director/designate of each UCCS *designated health care component* as well as the UCCS *security officer* to implement policies and procedures that, based upon the UCCS *designated health care component's* access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.
   B. It is the responsibility of the director/designate of each UCCS *designated health care component* as well as the UCCS *security officer* and the UCCS OIT to develop and implement procedures to establish, document, review and modify a user's access to *ePHI*. Access shall use the principle of "least privileges." For purposes of this document, "least privileges" means giving a user account only those privileges which are essential to perform its intended function.
   C. It is the responsibility of the director/designate of each UCCS *designated health care component* as well as the UCCS *security officer* to ensure procedures include aregular

review of those with access to *ePHI*, including the appropriateness of access levels. The period for which and the extent, frequency, and nature of reviews are determined by the UCCS *designated health care component's* security environment and overall security management process. The UCCS *security officer* will determine the period of review at least annually.

D. It is the responsibility of the director/designate of each UCCS *designated health care component* as well as the UCCS *security officer* and the UCCS OIT to ensure procedures must require prompt initiation of account modifications/termination.

5. Termination Procedures.
   A. It is the responsibility of the director/designate of each UCCS *designated health care component* as well as the UCCS OIT in conjunction with the Department of Human Resources to implement procedures for terminating access to *ePHI* when the employment of a workforce member ends.
   B. It is the responsibility of the director/designate of each UCCS *designated health care component* as well as the UCCS *security officer* to establish account maintenance procedures that ensure termination of accounts or change in access privileges for individuals who have been terminated or are no longer authorized to access *ePHI*.
6. Documentation. All documentation required by this policy must be retained for a period of six (6) years from when it was created or was last in effect, whichever is later.

Related Policies

APS 2027 Code of Conduct
APS 6005 IT Security Program
APS 6010 Data Governance
Reporting and filing a complaint (see Compliance and Ethics Website)
UCCS Policy 300-022 Employment Background Checks

Reference

45 CFR § 164.308(a)(3)
The Health Information Technology for Economic and Clinical Health Act (HITECH Act) National Institute for Standards and Technology ("NIST")

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

HIPAA Security Reminders Policy
Attachment 15

Scope of Policy

This policy governs the creation and implementation of security reminders for UCCS and its *designated health care components*. All *workforce members* of UCCS *designated health care components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated health care components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

1. It is the Policy of UCCS and its *designated health care components* to develop or acquire and to use appropriate information security reminders, or other information security awareness resources, on a regular basis.
2. The UCCS *privacy officer* and UCCS *security officer* shall assume responsibility for developing or acquiring such reminders and resources, and for implementing a plan and program ensuring their frequent use.
3. It is the Policy of UCCS and its *designated health care components* to document all information security reminder-related activities and efforts in accordance with HIPAA regulations.
4. The frequent use of appropriate security reminders and other information security awareness resources can reduce the likelihood of data breaches and HIPAA violations

Procedures

1. It is the responsibility of the director/designate of each UCCS *designated health care component* as well as the UCCS *security officer* to establish security awareness and HIPAA training for all UCCS *workforce members* involved in the creation, transmission, and storage of *ePHI*. Training activities include:
   A. Initial security awareness and HIPAA training for individuals with *ePHI*-related job duties. Training will include UCCS Password Standards and the importance of protecting against malicious software and exploitation of vulnerabilities.
   B. Review of changes to internal policies, procedures, and technologies.
   C. Periodic reminders about security awareness and HIPAA.
   D. Security notices or updates regarding current threats.
2. It is the responsibility of the director/designate of each UCCS *designated health care component* as well as the UCCS *security officer* to ensure HIPAA entities must maintain records of training materials and completion of training for six years.

Related Policies

APS 2027 Code of Conduct
APS 6002 Electronic Communications
APS 6005 IT Security Program
APS 6010 Data Governance
Reporting and filing a complaint (see Compliance and Ethics Website)
UCCS Policy 700-001 Email as Official Means of Communication
UCCS Policy 800-002 Social Media Policy

Reference

45 CFR § 164.308(a)(5)

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

HIPAA Malware Protection Policy
Attachment 16

Scope of Policy

This policy governs malware protection for UCCS *designated health care components*. All *workforce members* of UCCS *designated health care components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated health care components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

1. It is the Policy of UCCS and its *designated health care components* to develop and apply a rigorous program of techniques, technologies, and methods to guard against, detect, and report the presence of malicious software.
2. The use of appropriate techniques, technologies, and methods to protect information systems from malicious software ("malware") is a proven approach to reducing the likelihood of data breaches, system malfunctions, and HIPAA violations.
3. Responsibility for malware protection shall reside with the UCCS *security officer*, who shall ensure that the most effective and appropriate techniques, technologies, and methods are continuously used to protect our information systems, and the individually identifiable *health information* they contain, from malicious software.
4. It is the Policy of UCCS and its *designated health care components* to fully document all malware protection-related activities and efforts, in accordance with our documentation policy.

Procedures

1. It is the responsibility of the UCCS *security officer*, in conjunction with the UCCS Office of Information Technology (OIT) to protect all devices against malicious software, such as computer viruses, Trojan horses, and spyware. It is the responsibility of the UCCS *security officer*, in conjunction with the UCCS OIT to also ensure the safeguards and appropriate configurations are included in the standard set-up procedures for new systems and workstations that contain or access *electronic protected health information (ePHI)*.
2. It is the responsibility of the UCCS *security officer*, in conjunction with the UCCS OIT, to run versions of operating systems and application software for which security patches are made available and installed in a timely manner in accordance with UCCS Security Standards for Information Systems. The UCCS *security officer* will determine the period of review at least annually.
3. It is the responsibility of the UCCS *security officer*, in conjunction with the UCCS OIT, to "harden" systems. "Hardening" includes:

A. Installing OS and third-party application updates (patches) and keeping them current.
B. Changing or removing default logins/passwords.
C. Disabling unnecessary services.
D. Installing virus and malware protection software and updating them at least weekly.
E. Setting proper file/directory ownership/permissions.

4. It is the responsibility of the UCCS *security officer*, in conjunction with the UCCS OIT to periodically, and at least annually, review HIPAA workstation settings to ensure that they comply with UCCS Security Standards for Information Systems and UCCS Policy 700-002 Responsible Computing Section II.B.1.a.
5. It is the responsibility of the UCCS *security officer*, in conjunction with the UCCS OIT, to perform periodic network vulnerability scans of systems containing known *ePHI*, and workstations that access *ePHI*, and take adequate steps to correct discovered vulnerabilities.
6. It is the responsibility of the UCCS *security officer*, in conjunction with the UCCS OIT, to implement e-mail malicious code filtering.
7. It is the responsibility of the UCCS *security officer*, in conjunction with the UCCS OIT, to install/ enable firewalls (hardware and/or software) to reduce threat of unauthorized remote access.
8. It is the responsibility of the UCCS *security officer*, in conjunction with the UCCS OIT to ensure intrusion detection software and/or systems may also be installed to detect threat of unauthorized remote access.

Related Policies

APS 6002 Electronic Communications
APS 6005 IT Security Program
APS 6010 Data Governance
Reporting and filing a complaint (see Compliance and Ethics Website)
UCCS Policy 700-001 Email as Official Means of Communication
UCCS Policy 700-005 Computer Security Incident Response

Reference

45 CFR § 164.308(a)(5)
The Health Information Technology for Economic and Clinical Health Act (HITECH Act) National Institute for Standards and Technology ("NIST")

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

HIPAA Password Management Policy
Attachment 17

Scope of Policy

This policy governs information systems password management for UCCS *designated health care components*. All *workforce members* of UCCS *designated health care components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated health care components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

1. It is the Policy of UCCS and its *designated health care components* to require the use of strong passwords by all *workforce members* who access, use, or maintain systems that contain, transmit, receive, or use individually identifiable *health information*.
2. Individuals who access *protected health information (PHI)* are responsible for choosing passwords that adhere to the password procedures defined by the software system administrator and the referenced HIPAA best practices.

Procedures

1. It is the responsibility of the director/designate of each UCCS *designated health care component*, as well as the UCCS *security officer*, in conjunction with the UCCS Office of Information Technology (OIT), to ensure compliance with procedures for creating, changing, and safeguarding passwords.
2. It is the responsibility of each UCCS *designated health care component's* leadership, as well as the UCCS *security officer* to enforce password strength requirements for access by third-party access, when possible.
3. It is the responsibility of the director/designate of each UCCS *designated health care component*, as well as the UCCS *security officer*, to ensure that *workforce members* understand password procedures.
4. All *workforce members* must follow password management best practices as emphasized in HIPAA training programs, security reminders, and HIPAA awareness resources used by this organization.
5. In the event of a known information system compromise, some or all *workforce-member* passwords must be changed. This determination shall be made by the UCCS *security officer*.
6. Any *workforce member* who experiences any compromise of their password or pass-phrase shall follow the requirements in Attachment 5 Breach Notification Policy.

Related Policies

APS 6002 Electronic Communications
APS 6005 IT Security Program
APS 6010 Data Governance
Reporting and filing a complaint (see Compliance and Ethics Website)
UCCS Policy 700-001 Email as Official Means of Communication
UCCS Policy 700-002 Responsible Computing
UCCS Policy 700-003 Information Technology Security
UCCS Policy 700-005 Computer Security Incident Response

Reference

45 CFR § 164.308(a)(5)
45 CFR § 164.306

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

HIPAA Security Incident Policy
Attachment 18

Scope of Policy

This policy governs responses to security incidents involving the breach or compromise of *protected health information (PHI)* for UCCS *designated health care components*. All *workforce members* of UCCS *designated health care components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated health care components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

1. It is the Policy of UCCS and its *designated health care components* to rapidly identify and appropriately respond to all security incidents, regardless of their severity.
2. Responsibility for responding to and managing security incidents shall reside with the UCCS *security officer* and, if necessary, the UCCS *privacy officer*.
3. It is the responsibility of each UCCS *designated health care component's* leadership, as well as the UCCS *security officer*, in conjunction with UCCS Office of Information Technology (OIT), to develop procedures for Incident Response related to *electronic PHI (ePHI).*
4. It is the Policy of UCCS and its *designated health care components* to fully document all security incidents and responses, in accordance with UCCS documentation procedures and HIPAA requirements.

Procedures

1. Security Incident. A security incident or *breach* is an attempted or successful acquisition, unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system in a manner not permitted under the HIPAA Security Rule which compromises the security or privacy of the *PHI*.
2. Response and Reporting. UCCS is required to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of known incidents; and document incidents and their outcomes. This includes improper network activity and misuse of outside data.
   A. Suspected Incident Occurs. A security incident may occur through a misuse of UCCS OIT resources that results in a widespread intentional or unintentional compromise of information security. Also, large scale intrusions into a computing network may lead to unauthorized access to sensitive information and a lost or stolen laptop may result in a security incident involving sensitive data.
   B. Incident Detected. Incidents may be detected through many different means, with varying levels of detail. Automated detection capabilities include network-based and host-based

intrusion detection systems, antivirus software, and log analyzers. Incidents may also be detected through manual means, such as problems reported by users. While some incidents have overt signs that can be easily detected, others are almost impossible to detect without automation.

C. Do Not Disturb. No one is to disturb implicated data or devices. The incident may require further investigation. It is important that nothing be disturbed at this step of the procedure.

D. Report. Anyone who suspects that a privacy or security incident or *breach* has occurred is to report incidents to:
   1. The director/designate of the affected UCCS *designated health care component*;
   2. The UCCS *privacy officer* at comply@uccs.edu ; and
   3. The UCCS *security officer* at security@uccs.edu.

E. Mitigate – if possible, mitigate any harmful effects of the incident that are known. This may mean removing the affected device(s) from the network.

F. Categorize Incident. It is the responsibility of the director/designate of each UCCS *designated health care component* and the UCCS *security officer* to categorize the incident as:
   1. "Denial of Service" is an attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources such as central processing units (CPU), memory, bandwidth, and/or disk space.
   2. "Malicious Code" refers to a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the security or integrity of the victim's data. Malicious code is usually designed to perform these inappropriate functions without the user's knowledge. Viruses, worms, and Trojan horses are considered forms of malicious code.
   3. "Unauthorized Access" occurs when a person gains logical or physical access without permission to a network, system, application, data, or other resource. Unauthorized access is typically gained through the exploitation of operating system or application vulnerabilities, by getting hold of usernames and passwords, or social engineering.
   4. "Inappropriate Usage" occurs when a legitimate user violates acceptable computing use policies. Examples of inappropriate use include sending spam promoting a personal business, sending email perceived as harassing individuals, etc. Inappropriate use issues may not constitute a security incident but must be assessed by the UCCS *security officer* to determine if the inappropriate usage has created a security incident.
   5. "Multiple Component" is a single incident that encompasses two or more incidents or falls into multiple incident categories. These incidents should be handled in line with the severest infraction involved.

G. Investigate and Respond to Incident. It is the responsibility of the UCCS *security officer* in conjunction with UCCS OIT to investigate and respond to the incident and mitigate any harmful effects of the incident, if possible.
   1. If the incident cannot be handled by the UCCS *security officer* and/or UCCS OIT, the UCCS *security officer* will call an ad hoc meeting of appropriate individuals to make up an incident response team to investigate and respond to the incident. The ad hoc group may be composed of some or all of the following members or their representatives, as determined by the UCCS *security officer* to appropriately respond to the incident:
      a. Assistant Vice Chancellor for Information Technology and Chief Information Officer
      b. Registrar (if student data);
      c. Human Resources;
      d. UCCS Legal Counsel;
      e. UCCS Office of Compliance;

f. Vice Chancellor of affected unit;
g. Dean, Director, Chair, or Head of affected unit;
h. Public Relations;
i. Campus Police;
j. Appropriate Office of Information Technology personnel;
k. UCCS *Privacy Officer*;
l. Others, as determined by the UCCS *security officer*.

2. If the incident is of significant magnitude, the following members should be considered by the UCCS *security officer* for inclusion in the group:
   a. Internal Audit;
   b. CU-System Legal Counsel;
   c. CU-System Public Relations;
   d. Other CU Campus Information Technology or OIT Offices;
   e. Risk Management.

H. Documentation. It is the responsibility of the director/designate of each UCCS *designated health care component*, as well as the UCCS *security officer* to ensure that the incident, investigation, response, and outcome is properly documented. The UCCS *security officer*, UCCS OIT, and/or the response team must document the security incident, investigation of the incident, and response and remediation. The UCCS *security officer* is responsible for retaining documentation of incidents.

I. Conclusion. The UCCS *security officer*, UCCS OIT, and/or the response team should determine if policies or procedures need to be implemented to prevent a reoccurrence of the incident or if additional campus education or purchase of network or computing security devices are needed to prevent similar future incidents.

3. Additional Documentation.
   A. All breach notification activities will be managed by the UCCS *privacy officer* and the UCCS *security officer* who will report to the Office of Civil Rights with the assistance and cooperation of involved UCCS staff and departments. This includes notice to affected individuals and to the Secretary of Health and Human Services and the Office of Civil Rights.
   B. Security incident procedure documentation and changes shall be retained for six (6) years.

Related Policies

APS 2027 Code of Conduct
APS 6002 Electronic Communication
APS 6005 IT Security Program
APS 6010 Data Governance
Reporting and filing a complaint (see Compliance and Ethics Website)
UCCS Policy 300-022 Employment Background Checks
UCCS Policy 700-001 Email as Official Means of Communication
UCCS Policy 700-004 Wireless Network
UCCS Policy 700-005 UCCS Computer Security Policy

Reference

45 CFR § 164.308(a)(6)
45 CFR § § 164.400 to 164.414

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

Data Backup and Storage Policy
Attachment 19

Scope of Policy

This policy governs data backup and storage for UCCS *designated health care components*. All *workforce members* of UCCS *designated health care components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated health care components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

1. It is the Policy of UCCS and its *designated health care components* to create and maintain complete, retrievable, exact backups of all individually identifiable *health information* generally, and *electronic protected health information (ePHI)* specifically, held, processed, or stored in the course of business operations, in full compliance with all the requirements of HIPAA.
2. All data backups shall be created and maintained in such manner as to ensure that the maximum degree of data integrity, availability, and confidentiality are maintained at all times.
3. The storage of data backups in a separate location, removed from normal business operations (offsite) is an essential element of any successful data backup plan.
4. Backups help to ensure that healthcare providers and others have immediate, around-the-clock access to patient information.
5. It is the Policy of UCCS and its *designated health care components* to create retrievable, exact copies of *ePHI*, when needed, before any movement or maintenance of data processing equipment that could result in the loss or compromise of *ePHI*.
6. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to perform appropriate backups on UCCS *designated health care component's* network, including shared drives containing application data, patient information, financial data, and crucial system information.
7. The ability to create and maintain retrievable, exact copies of individually identifiable *health information* generally, and *ePHI* specifically, is a critical element of our business operations and our ability to respond to unexpected negative events.
8. Timely access to *health information* is crucial to providing high quality health care, and to our business operations.

Procedures

1. <u>Data Backup</u>
   A. It is the responsibility of the director/designate of each UCCS *designated health care component* to ensure the back up of original sources of essential *ePHI* is done on an established schedule.

B. It is the responsibility of the director/designate of each UCCS *designated health care component* to ensure backup copies are securely stored in a physically separate location from the data source.
C. It is the responsibility of the director/designate of each UCCS *designated health care component* to ensure backups containing *ePHI* will be transported via secure methods.
D. It is the responsibility of the director/designate of each UCCS *designated health care component* to ensure documentation exists to verify the creation of backups and their secure storage.

2. Accountability.
   A. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to maintain a record of the movements of hardware and electronic media and any person responsible therefore.
   B. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to maintain a record of the movements of, and individual(s) responsible for, hardware and electronic media containing *ePHI*.
      1. The record(s) should identify all types of hardware and electronic media that must be tracked.
         i. Special attention must be paid to portable devices and removable media. These devices should not ordinarily contain *ePHI* and must be individually identified in the tracking system in order to contain *ePHI*. Their use must be consistent with the individual's identified role, such as according to a role-based matrix.
         ii. This inventory should be physically confirmed at least annually.
      2. The tracking system must include a mechanism for documenting the initial assignment of responsibility for devices that contain *ePHI*, as well as the transfer of authority for these devices.
   C. Transport of archival media between the origination point and remote storage location must use a secure method to avoid unauthorized access to the archival media.
   D. Loss or theft of electronic equipment or media containing *ePHI* must immediately be reported according Attachment 18 Security Incident Policy.

3. Data backup and storage.
   A. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to create a retrievable, exact copy of *ePHI*, when needed, before movement of equipment.
   B. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to create a retrievable, exact copy of original sources of essential *ePHI* before moving equipment containing them.
   C. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to establish a process for documenting or verifying creation of retrievable, exact copy of original sources of essential *ePHI*.
   D. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to develop retrievable, exact copies of *ePHI* that must be protected in accordance with these Standards.

Related Policies

APS 6005 IT Security Program
APS 6010 Data Governance

Reporting and filing a complaint (see Compliance and Ethics Website)

Reference

45 CFR § 164.308(a)(7)
45 CFR § 164.310(a)(1-2)
45 CFR § 164. 164.310(d)(2)(iii)

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

HIPAA Disaster Recovery Policy
Attachment 20

Scope of Policy

This policy governs contingency disaster recovery planning for UCCS *designated health care components*. All *workforce members* of UCCS *designated health care components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated health care components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

1. It is the Policy of UCCS and its *designated health care components* to establish and implement processes and procedures to create and maintain procedures for recovery of *electronic protected health information (ePHI)* and associated technology in the event of adisaster.
2. A disaster may occur at any time, not necessarily during work hours.
3. UCCS *designated health care components* must make reasonable efforts to remain operational with as little disruption of business operations and patient care as possible.
4. Continuity of patient care requires uninterrupted access to patient information.
5. In a dangerous emergency, evacuating personnel has priority over preserving information assets.
6. The following conditions can destroy or disrupt UCCS *designated health care components* information systems: power interruption, fire, water, weather and other natural phenomena, sabotage, and vandalism.

Procedures

1. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to establish procedures to restore loss of essential *ePHI* (and hardcopy *PHI*) as a result of a disaster or emergency.
2. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to maintain copies of the data restoration procedures that are readily accessible at more than one location and should not rely on the availability of local power or network.
3. It is the responsibility of the director/designate of each UCCS *designated health care component* and the UCCS *security officer* to ensure that backup procedures include steps to ensure that all protections (patches, configurations, permissions, firewalls, etc.) are re-applied and restored before *ePHI* is restored to a system.
4. The UCCS director of emergency management should be contacted as appropriate.

Related Policies

APS 2027 Code of Conduct
APS 6005 IT Security Program
APS 6010 Data Governance
Reporting and filing a complaint (see Compliance and Ethics Website)
UCCS Public Safety Website

Reference

45 CFR § 164.308(a)(7)

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

Emergency Mode Operations Policy
Attachment 21

Scope of Policy

This policy governs emergency mode operations and planning for UCCS *designated health care components*. All *workforce members* of UCCS *designated health care components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated health care components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

1. It is the Policy of UCCS and its *designated health care components* to establish this emergency mode operations policy to implement procedures to enable continuation of critical business processes for the protection of individually identifiable *health information* while operating in emergency mode.
2. This emergency mode operations policy is designed to ensure the protection and availability of individually identifiable *health information* and *protected health information (PHI)* during emergencies requiring UCCS *designated health care components* to operate in "emergency mode".
3. UCCS *designated health care components* must comply with HIPAA and the HIPAA implementing regulations pertaining to emergency mode operations planning, in accordance with the requirements at § 164.308(a)(7).
4. Individually identifiable *health information* must be protected during emergencies, even as it is protected during normal operations.
5. The University's emergency mode operations plan must be implemented and executed by the director/designate of each UCCS *designated health care component* in conjunction with other emergency and/or disaster plans and procedures, as appropriate and necessary.
6. It is the Policy of UCCS and its *designated health care components* to fully document all emergency planning and preparedness activities and efforts.

Procedures

1. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to ensure that HIPAA entity emergency operations procedures maintain security protections for *ePHI*.
2. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to evaluate operations in emergency mode, like a technical failure or power outage, to determine whether security processes to protect *ePHI* are maintained.
3. It is the responsibility of the director/designate of each UCCS *designated health care component* to document assessment and conclusions.

4. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to document and implement additional authorities and procedures necessary to ensure the continuation of security protections for *ePHI* during emergency operations mode.
5. It is the responsibility of the director/designate of each UCCS *designated health care component* to develop plans for evacuations.
    a. Each UCCS *designated health care component's* emergency response plan shall include logging out of systems that contain *ePHI*, securing files, and locking up before evacuating a building, if safe to do so.
    b. UCCS *designated health care components* should have processes to ensure there was no breach when the area is re-occupied.
6. The UCCS director of emergency management should be contacted as appropriate.

Related Policies

APS 2027 Code of Conduct
APS 6005 IT Security Program
APS 6010 Data Governance
Reporting and filing a complaint (see Compliance and Ethics Website)
UCCS Public Safety Website

Reference

45 CFR § 164.308(a)(7)

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

Policy on Testing and Revision of Contingency and Emergency Plans and Procedures
Attachment 22

Scope of Policy

This policy governs testing and revision of contingency and emergency plans and procedures for UCCS and its *designated health care components.* All *workforce members* of UCCS *designated health care components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated health care components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

1. It is the Policy of UCCS and its *designated health care components* to periodically test and revise, as necessary, all emergency preparedness plans, including emergency and contingency plans.
2. UCCS *designated health care components* must comply with HIPAA and the HIPAA implementing regulations pertaining to the testing and revision of emergency and contingency plans and procedures, in accordance with the requirements at § 164.308(a)(7).
3. Emergency and contingency plans, and the procedures associated with them, must be periodically tested and revised to ensure that they meet the emergency preparedness needs of UCCS *designated health care components*.
4. It is the Policy of UCCS and its *designated health care components* that all individually identifiable *health information*, including *protected health information (PHI)*, shall be afforded the same degree of security and privacy protection during the execution of any emergency or contingency plan as such information would receive during normal business operations.

Procedures

1. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to implement procedures for periodic testing and revision of contingency plans.
2. It is the responsibility of the director/designate of each UCCS *designated health care component* to document the contingency plan procedures.
3. It is the responsibility of the director/designate of each UCCS *designated health care component* to ensure that those responsible for executing contingency plan procedures understand their responsibilities.
4. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to periodically, and at least annually, perform a test of the contingency plan procedures.

5. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to document test results, review and correct any problems with the test, and update procedures accordingly.
6. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to ensure that individually identifiable *health information*, including *PHI*, must be afforded the same degree of security and privacy protection during the execution of any emergency or contingency plan as such information would receive during normal business operations.

Related Policies

APS 2027 Code of Conduct
APS 6005 IT Security Program
APS 6010 Data Governance
Reporting and filing a complaint (see Compliance and Ethics Website)
UCCS Public Safety Website

Reference

45 CFR § 164.308(a)(7)

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

Policy on Applications and Data Criticality Analysis
Attachment 23

Scope of Policy

This policy governs data and applications criticality analyses for UCCS *designated health care components*. All *workforce members* of UCCS *designated health care components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated health care components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

1. It is the Policy of UCCS and its *designated health care components* to assess the relative criticality of all data, as defined by the UCCS *security officer*, so that such data may be properly protected during emergencies and during normal business operations.
2. UCCS *designated health care components* must comply with HIPAA and the HIPAA implementing regulations pertaining to the analysis of the relative criticality of both data and applications, in accordance with the requirements at § 164.308(a)(7).
3. A thorough assessment and understanding of the relative criticality of both data and applications is essential to emergency preparedness, and to effectively protecting individually identifiable *health information*, including *protected health information (PHI)* during emergencies and during normal business operations.

Procedures

1. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to prioritize criticality of applications and data sets for data back-up, restoration, and application of emergency mode operation plan.
2. Priorities can be included in data restoration procedures, see Attachment 20 Disaster Recovery Policy.

Related Policies

APS 2027 Code of Conduct
APS 6002 Electronic Communications
APS 6005 IT Security Program
APS 6010 Data Governance
Reporting and filing a complaint (see Compliance and Ethics Website)
UCCS Policy 300-022 Employment Background Checks
UCCS Policy 700-001 Email as Official Means of Communication
UCCS Policy 800-002 Social Media Policy

Reference

45 CFR § 164.308(a)(7)

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

Policy on Evaluating the Effectiveness of Security Policies and Procedures Attachment 24

Scope of Policy

This policy governs periodic evaluations of the effectiveness of security policies and procedures for UCCS *designated health care components*. All *workforce members* of UCCS *designated health care components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated health care components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

1. It is the Policy of UCCS and its *designated health care components* to periodically evaluate security policies and procedures, including emergency and contingency plans and procedures, in order to improve their effectiveness.

Procedures

1. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* and the UCCS *privacy officer* to review and update their HIPAA related policies and practices for compliance every five (5) years, or more frequently in response to environmental or operational changes that affect the security of *electronic protected health information (ePHI).*

   A. The director/designate of each UCCS *designated health care component* shall submit to the UCCS *security officer* and the UCCS *privacy officer* once annually by calendar year-end a list of titles and last revision dates of the policies designed to meet HIPAA Privacy and Security Rule requirements and provide copies upon request.

2. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* and the UCCS *privacy officer* to review and update unit policies and procedures annually if there is no trigger for more frequent review.

3. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* and the UCCS *privacy officer* to identify the individual(s) responsible for determining when evaluation is necessary due to environmental or operational changes.

4. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* and the UCCS *privacy officer* to document periodic reviews the updates and archive previous versions of policies and retain for six years as per Attachment 2 Documentation Policy (Retention).

Related Policies

APS 2027 Code of Conduct
APS 6005 IT Security Program
Reporting and filing a complaint (see Compliance and Ethics Website)

Reference

45 CFR § 164.308(a)(8)

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

Business Associates Policy
Attachment 25

Scope of Policy

This policy governs relationships with, and operations involving *business associates* for UCCS *designated health care components*. All *workforce members* of UCCS *designated health care components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated health care components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

It is the Policy of UCCS and its *designated health care components* to establish and maintain business and working relationships with *business associates* that are in full compliance with all the requirements of HIPAA Final "Omnibus" Rule.

Procedures

1. Responsibility for maintaining appropriate and lawful relationships with *business associates* shall reside with each director/designate of a UCCS *designated health care component* in conjunction with the UCCS *privacy officer* and legal counsel, who shall ensure that: all aspects of the University's *business associate* relationships are appropriate; and individually identifiable *health information*, including *protected health information (PHI)*, as defined by HIPAA, is properly protected and safeguarded by our *business associates*.
2. Whenever possible the Business Associate Agreement (BAA) template form should be used and signed by the proper signatory with delegated authority pursuant to UCCS Policy 100-011 Managing and Executing University Contracts. If the BAA template is not used, the director/ designate of the UCCS *designated health care component* must send the BAA to the UCCS *privacy officer* and legal counsel for review and approval.
3. With regard to *business associates*, the duties and responsibilities of each director/designate of UCCS *designated health care components*, in conjunction with the UCCS *privacy officer*, shall include, but are not limited to the following:
   A. Ensure that all *business associate* contracts meet all HIPAA requirements and standards, including those requirements and standards amended by the HITECH Act, the HIPAA "Omnibus" Final Rule, and any requirements Colorado state law. All *business associate* contracts must:
      1. Ensure that individually identifiable *health information*, including *PHI*, is properly protected and safeguarded by *business associates*.
      2. Ensure that *business associates* understand the importance and necessity of protecting individually identifiable *health information*, including *PHI*, whether in electronic form (*ePHI*) or hardcopy form.

3. Ensure that *business associates* have proper and appropriate safeguards in place for individually identifiable *health information*, including *PHI*, before entrusting such information to them.
4. Ensure that *business associates* understand and are properly prepared to detect and respond to breaches of individually identifiable *health information*, including *PHI*.

4. In cooperation with the University, *business associates* may work with, use, transmit, and/or receive individually identifiable *health information*, including *PHI*, which is afforded specific protections under HIPAA.
5. Each director/designate of UCCS *designated health care components* has the primary responsibility in all *business associate* relationships to ensure that individually identifiable *health information*, including *PHI*, is properly protected and safeguarded.
6. The HIPAA ("Omnibus") Final Rule specifically identifies the following types of entities as potential *business associates*:
   A. Subcontractors
   B. Patient safety organizations.
   C. Health Information Organizations (HIOs) and similar organizations. Health and Human Services declined to specifically define HIOs in the Omnibus Rule but chose the term "HIO" because it includes both Health Information Exchanges (HIEs) and regional health information organizations.
   D. E-Prescribing gateways.
   E. Personal Health Record (PHR) vendors that provide services on behalf of a covered entity. PHR vendors that do not offer PHRs on behalf of UCCS *designated health care components* are not *business associates*.
   F. Other firms or persons who "facilitate data transmission" that requires routine access to *PHI*.
7. The *minimum necessary standard* now applies directly to *business associates* and their subcontractors. When using, disclosing or requesting *PHI*, all these entities must make reasonable efforts to limit *PHI* to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.
8. Subcontractors of *business associates* are now *business associates* themselves. A subcontractor is defined as a person or entity to whom a *business associate* delegates a function, activity, or service involving *PHI*, and who is not a member of the *business associate's* own workforce. UCCS *designated health care components* are not required to enter into a contract or other arrangement with a *business associate* that is a subcontractor. That is the responsibility of the primary or first-tier *business associate*.
9. Each director/designate of UCCS *designated health care components* shall fully document all *business associate*-related contracts and activities, in accordance with our Attachment 2 HIPAA-Related Documentation Policy and the requirements of HIPAA.

Related Policies

APS 2027 Code of Conduct
APS 6002 Electronic Communications
APS 6005 IT Security Program
APS 6010 Data Governance
Reporting and filing a complaint (see Compliance and Ethics Website)
UCCS Policy 100-011 Managing and Executing University Contracts
UCCS Policy 300-022 Employment Background Checks
UCCS Policy 700-001 Email as Official Means of Communication

Reference

45 CFR § 164.308(b)(1)
45 CFR § 164.410
45 CFR § 164.502(e)
45 CFR § 164.504(e)

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

Contingency Operations Policy
Attachment 26

Scope of Policy

This policy governs contingency operations planning and implementation for UCCS *designated health care components*. All *workforce members* of UCCS *designated health care components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated health care components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

1. It is the Policy of UCCS and its *designated health care components* to be fully prepared to protect individually identifiable *health information*, including *protected health information (PHI)* and *electronic PHI (ePHI)*, during emergencies and contingency operations.
2. Contingency Operations, for purposes of this policy document, are defined as processes and procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
3. Contingency Operations plans and procedures, in combination with other emergency preparedness plans and procedures, shall be documented, analyzed, revised, and updated periodically in accordance with other established emergency preparedness and documentation policies and procedures.
4. Responsibility for planning and executing contingency operations shall reside with the director/designate of each UCCS *designated health care component*, who shall prepare, analyze, test, and update plans for contingency operations on a periodic basis.
5. It is the Policy of UCCS *designated health care components* to fully document all contingency operations plans and procedures.

Procedures

1. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer*, to establish, and implement as needed, procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
2. It is the responsibility of the director/designate of each UCCS *designated health care component* to ensure that contingency procedures and authorization are documented, see Attachment 27 Facility Security Policy.

Related Policies

APS 2027 Code of Conduct

APS 6002 Electronic Communications
APS 6005 IT Security Program
APS 6010 Data Governance
Reporting and filing a complaint (see Compliance and Ethics Website)

Reference

45 CFR § 164.310(a)(1-2)

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

Facility Security Policy
Attachment 27

Scope of Policy

This policy governs facility security for UCCS *designated health care components*. All *workforce members* of UCCS *designated health care components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated health care components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

1. It is the Policy of UCCS and its Designated Health Care Components to provide facility security, in addition to other technical and administrative safeguards, in order to provide protection for individually identifiable *health information*, including *protected health information* (*PHI*).
2. In addition to other technical and administrative safeguards, strong facility security is an essential element of our efforts to provide protection for individually identifiable *health information*, including *PHI*.

Procedures

1. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer*, UCCS *privacy officer*, and UCCS Facilities Services Department to implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
2. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to ensure systems and electronic media containing *PHI* are located in physically secure locations. A secure location would minimally be defined as one that is not routinely accessible to the public, particularly if authorized personnel are not always available to monitor security.
3. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS Facilities Services Department to ensure that secure locations have physical access controls (card key, door locks, alarms, etc.) that prevent unauthorized entry, particularly during periods outside of normal work hours, or when authorized personnel are not present to monitor security. If logging is available, it should be enabled.
4. It is the responsibility of the UCCS Facilities Services Department in conjunction with the UCCS *security officer* to ensure access to control systems are maintained in good working order.

Related Policies

APS 6005 IT Security Program

APS 6010 Data Governance
Reporting and filing a complaint (see Compliance and Ethics Website)

Reference

45 CFR § 164.310(a)(1-2)
The Health Information Technology for Economic and Clinical Health Act (HITECH Act)
National Institute for Standards and Technology ("NIST")

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

Access Control and Validation Policy
Attachment 28

Scope of Policy

This policy governs access control and validation for UCCS *designated health care components*. All *workforce members* of UCCS *designated health care components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated health care components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

1. It is the Policy of UCCS and its *designated health care components* to implement and support strong and ongoing access control and validation procedures, in full compliance with all the requirements of HIPAA.
2. Access control and validation procedures are designed to control and validate individualaccess to facilities based on role or function; including visitor control and access control for software testing and revision.
3. Strong access control and validation procedures are an essential element of protecting individually identifiable *health information*, including *protected health information(PHI)*.

Procedures

1. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* and the UCCS *privacy officer* to implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
2. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to develop an access plan for facilities containing *electronic PHI (ePHI)* that utilizes role- or function-based access control, including for visitors, service providers, and contractors.
3. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to ensure the role- or function-based access control and validation procedures are closely aligned with the facility security plan.
4. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to ensure the security plan for facilities containing *ePHI* includes key systems or electronic door access.
5. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer*, the UCCS *privacy officer*, the UCCS Department of Facility Services, and the UCCS Department of Human Resources to conduct a periodic (atleast

annual) review and implementation of termination procedures, which may include a review of key inventory or electronic door access, to ensure currency of access authorization.

Related Policies

APS 6005 IT Security Program
APS 6010 Data Governance
Reporting and filing a complaint (see Compliance and Ethics Website)

Reference

45 CFR § 164.310(a)(1-2)
The Health Information Technology for Economic and Clinical Health Act (HITECH Act) National Institute for Standards and Technology ("NIST")

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

Facility Security Maintenance Records Policy
Attachment 29

Scope of Policy

This policy governs the disposition of records pertaining to maintenance of the physical security of UCCS *designated health care components* facilities. All *workforce members* of UCCS *designated health care components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated health care components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

1. It is the Policy of UCCS and its *designated health care components* to create and maintain complete facility security maintenance records, in full compliance with all the requirements of HIPAA.
2. Facility security maintenance records are created to document repairs and changes to physical elements of a facility related to security.
3. It is the Policy of UCCS and its *designated health care components* to fully document facility security maintenance records-related activities and efforts.

Procedures

1. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS Facility Services Department to implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security, such as hardware, walls, doors, and locks.
2. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS Facility Services Department to develop policies and procedures for maintaining a record of any maintenance repairs and modifications to physical components of a facility containing *electronic protected health information (ePHI)* related to security, such as hardware, walls, doors, and locks.
    A. Documentation should contain appropriate detail for review, including date, repair, and/or modification(s) made, and the contractor's name and contact information.
    B. Documentation should be stored securely.
3. It is the responsibility of each UCCS *designated health care component's* leadership in conjunction with the UCCS Facility Services Department to identify individual(s) responsible for recording and maintaining these records.

Related Policies

APS 6005 IT Security Program
APS 6010 Data Governance
Reporting and filing a complaint (see Compliance and Ethics Website)

Reference

45 CFR § 164.310(a)(1-2)
The Health Information Technology for Economic and Clinical Health Act (HITECH Act) National Institute for Standards and Technology ("NIST")

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

Workstation Use and Security Policy
Attachment 30

Scope of Policy

This policy governs information use and security for UCCS *designated health care components*. All *workforce members* of UCCS *designated health care components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated health care components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

1. It is the Policy of UCCS and its *designated health care components* to configure, operate, and maintain our information workstations in full compliance with all the requirements of HIPAA.
2. UCCS's objective in these efforts is to provide reasonable protections for individually identifiable *health information*, including *protected health information (PHI).*
3. Specific procedures shall be developed to specify the proper functions, procedures, and appropriate environments of workstations that access individually identifiable *health information*, including *PHI*.
4. Responsibility for the development and implementation of this workstation security policy, and any procedures associated with it, shall reside with the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer*, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
5. Specific procedures shall be developed to implement physical safeguards for all workstations that access individually identifiable *health information*, including *PHI*, to restrict access to authorized users only.
6. It is the Policy of UCCS and its *designated health care components* to fully document all workstation-use-related activities and efforts, in accordance with the requirements of HIPAA.

Procedures

1. Workstation Use.
   A. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access *electronic PHI (ePHI).*
   B. Procedures for securing all UCCS workstations are defined by the UCCS Office of Information Technology (OIT) in UCCS Security Standards for Information Systems.

C. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to ensure functions to be performed on workstations containing or accessing *ePHI* are aligned with roles.
D. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to develop policies and procedures that specify where to place and position workstations to only allow viewing by authorized individuals, as well as additional privacy measures, commensurate with the risk of exposure.
E. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to ensure unencrypted *ePHI* will not be stored on portable electronic devices, including laptops.
F. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to ensure storage of *ePHI* on non-University equipment is forbidden, except in the case of storage by a third party with a HIPAA Business Associate Agreement.
G. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* and the UCCS OIT to ensure remote access of *ePHI* will utilize secure channels.
H. It is the responsibility of each *workforce member* to lock their computer when not in use and secure any *PHI* visible to non-workforce members.

2. Workstation Security
   A. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to ensure all workstations, including laptops, containing *ePHI* are to be physically secured, meaning locked down.
   B. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to ensure all workstations and electronic devices that contain or access *ePHI* will be identified, such as laptops, desktop computers, and personal digital assistants (PDAs).
   C. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to ensure unencrypted *ePHI* will not be stored on portable electronic devices, including laptops.
   D. If *ePHI* is stored on removable media, additional physical controls must be implemented, such as ensuring that the device is physically secured or in the physical possession of the responsible party. Encryption is a compensating control for these additional measures.

Related Policies

APS 2027 Code of Conduct
APS 6002 Electronic Communications
APS 6005 IT Security Program
APS 6010 Data Governance
Reporting and filing a complaint (see Compliance and Ethics Website)

Reference

45 CFR § 164.310(b-c)

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

Media Disposal and Re-Use
Hardware and Media Accountability Policy
Attachment 31

Scope of Policy

This policy governs media disposal and re-use for UCCS *designated health care components*. All *workforce members* of UCCS *designated health care components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated health care components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

1. It is the Policy of UCCS and its *designated health care components* to dispose of all media containing individually identifiable *health information*, including *protected health information (PHI)* and maintain records of the movements of hardware and electronic media, in full compliance with all the requirements of HIPAA.
2. Media containing individually identifiable *health information*, including *PHI*, must be completely erased, properly encrypted, or totally destroyed in its final disposition, or the data residing on such media is subject to recovery and subsequent misuse or theft.
3. It is the Policy of UCCS and its *designated health care components* to properly erase and/or sanitize ("wipe") all media containing individually identifiable *health information*, including *PHI*, before any media may be re-used.
4. Responsibility for proper media disposal and disposition shall reside with the director/designate of each UCCS *designated health care component*, who shall develop procedures to ensure the proper disposition of all such media.
5. Responsibility for proper media re-use shall reside with the director/designate of each UCCS *designated health care components*, who shall develop procedures to ensure the proper disposition of all such media before any re-use.
6. It is the Policy of UCCS and its *designated health care components* to maintain records of the movements of hardware and electronic media, and any person responsible therefore, in full compliance with all the requirements of HIPAA.
7. Responsibility for the development and implementation of this hardware and media accountability policy, and any procedures associated with it, shall reside with the director/designate of each UCCS *designated health care component*, who shall ensure that these procedures are maintained, updated as necessary, and implemented fully within the healthcare component.
8. Specific procedures shall be developed to ensure that UCCS maintains records of the movements of hardware and electronic media, and any person responsible therefore.

Procedures

1. Device and Media Disposal.
   A. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to implement policies and procedures to address the final disposition of *electronic PHI (ePHI)*, and/or the hardware or electronic media on which it is stored, see section 1.c below.
   B. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to ensure that *ePHI* on hardware and electronic media, including copiers, faxes, printers, etc., is unusable and/or inaccessible prior to disposal, including disposal by a *business associate* (Attachment 25 Business Associates).
   C. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to follow UCCS Policy 700-006 Computer and Electronics Disposal.
   D. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to ensure that when portable media is discarded, it must either be overwritten in accordance with National Institute of Standards and Technology (NIST) guidelines,http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf, or physically destroyed, eliminating all possibility that any *ePHI* contents could be read.
   E. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to ensure when a system is recycled, transferred to another user not authorized for the data, or discarded, all storage devices or all *ePHI* records must be overwritten in accordance with NIST guidelines (link above), or physically destroyed, rendering all *ePHI* records unreadable.
2. Media Re-Use.
   A. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to implement procedures for removal of *ePHI* from electronic media before the media are made available for re-use.
   B. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to ensure that *ePHI* on hardware and electronic media is unusable and/or inaccessible prior to re-use.
   C. When a system is recycled or transferred to another user not authorized for the data, or otherwise re-used outside of a HIPAA-compliant environment, all storage devices or all *ePHI* records must be overwritten in accordance with National Institute of Standards and Technology (NIST) guidelines,http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf, rendering all *ePHI* records unreadable.

Related Policies

APS 2027 Code of Conduct
APS 6005 IT Security Program
APS 6010 Data Governance
Reporting and filing a complaint (see Compliance and Ethics Website)
UCCS Policy 700-002 Responsible Computing
UCCS Policy 700-005 Computer Security Incident Response
UCCS Policy 700-006 Computer and Electronic Disposal

Reference

45 CFR § 164.310(a)(1-2)
The Health Information Technology for Economic and Clinical Health Act (HITECH Act)
National Institute for Standards and Technology ("NIST")

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

Unique User Identification Policy
Attachment 32

Scope of Policy

This policy governs the issuance, maintenance, and security of unique user identification's (ID's) for access to UCCS *designated health care components*. All *workforce members* of UCCS *designated health care components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated health care components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

1. It is the Policy of UCCS and its *designated health care components* to exclusively use unique user ID's for all information system access and activities, in full compliance with all the requirements of HIPAA.
2. Responsibility for the development and implementation of this unique user ID policy, and any procedures associated with it, shall reside with the director/designate of each UCCS *designated health care component*, who shall ensure that access to all UCCS information systems and data is accomplished exclusively through the use of unique user ID's.
3. Nothing in this policy shall limit the use of additional security measures, including login and access measures that may further enhance the security and protection UCCS provides to individually identifiable *health information*, including *protected health information (PHI)*.

Procedures

1. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to implement technical policies and procedures for electronic information systems that maintain *electronic PHI (ePHI)* to allow access only to those persons or software programs that have been granted access rights (Attachment 28 Access Control Validation Policy).
2. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to assign a unique name and/or number for identifying and tracking user identity.
3. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to provide a unique account, with a unique username/user ID and password, for access to *ePHI*.
4. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to assure shared accounts are not permitted for access to *ePHI*.

Related Policies

APS 6005 IT Security Program
APS 6010 Data Governance
Reporting and filing a complaint (see Compliance and Ethics Website)

Reference

45 CFR § 164.310(a)(1-2)

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

Emergency Access Policy
Attachment 33

Scope of Policy

This policy governs access to *protected health information (PHI)* during emergencies affecting UCCS *designated health care components*. All *workforce members* of UCCS *designated health care components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated health care components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

1. It is the Policy of UCCS and its *designated health care components* to establish and implement emergency access procedures, in full compliance with all the requirements of HIPAA.
2. These emergency access procedures apply to access to individually identifiable *health information*, including *PHI*.
3. Responsibility for the development and implementation of UCCS emergency access procedures shall reside with the director/designate of each UCCS *designated health care component*, who shall ensure that these procedures are maintained, updated as necessary, and implemented fully throughout their department.
4. Specific procedures shall be developed to ensure that authorized *workforce members* can access individually identifiable *health information*, including *PHI* during emergencies.
5. These emergency access procedures shall be developed and implemented in combination with our emergency preparedness and response plans.
6. It is the Policy of UCCS and its *designated health care components* to fully document our emergency access procedures development and implementation, in accordance with our Attachment 2 HIPAA-Related Documentation Policy and the requirements of HIPAA.

Procedures

1. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to establish (and implement as needed) procedures for obtaining necessary *electronic PHI (ePHI)* during an emergency.
2. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to establish procedures to ensure that necessary *ePHI* can be accessed during an emergency.
   A. Emergency access procedures may be included in contingency plan procedures (see Attachment 26 Contingency Operations Policy).
3. It is the responsibility of the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer* to develop emergency access procedures that shall be written and communicated in advance to all individuals in the department.

4. It is the responsibility of the director/designate of each UCCS *designated health care component* to ensure emergency access procedures should not rely on the availability of a single individual.
5. It is the responsibility of the director/designate of each UCCS *designated health care component* to ensure access to emergency procedures should not rely on the availability of local power or network.
6. It is the responsibility of the director/designate of each UCCS *designated health care component* to identify roles that may require special access during an emergency.
    A. Individuals are to require proper ID or other official verification before granting access to unknown or not-normally-authorized individuals in emergency circumstances.

Related Policies

APS 2027 Code of Conduct
APS 6005 IT Security Program
APS 6010 Data Governance
Reporting and filing a complaint (see Compliance and Ethics Website)

Reference

45 CFR § 164.104
45 CFR § 164.306
45 CFR § 164.312(a)(1)

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

Automatic Log-Off Policy
Attachment 34

Scope of Policy

This policy governs the implementation of automatic log-offs for UCCS *designated health care components*. All *workforce members* of UCCS *designated health care components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated health care components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

1. It is the Policy of UCCS and its *designated health care components* to always use automatic log-off applications or systems on all workstations and computers, in full compliance with the requirements of HIPAA.
2. Responsibility for the development and implementation of this automatic log-off policy, and any procedures associated with it, shall reside with the director/designate of each UCCS *designated health care component* in conjunction with the UCCS *security officer*, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout ourorganization.
3. Specific procedures shall be developed to specify the proper functions and procedures of our automatic log-off systems on all computers and workstations that access individually identifiable *health information*, including *protected health information (PHI)*.

Procedures

1. It is the responsibility of the UCCS *security officer* in conjunction with the director/designate of each UCCS *designated health care component* to implement electronic procedures that terminate an electronic session after a predetermined time of inactivity as per Attachment 38 Person or Entity Authentication Policy.
2. It is the responsibility of the UCCS *security officer* in conjunction with the director/designate of each UCCS *designated health care component* to ensure, where possible, that electronic sessions terminate after a period of inactivity.
3. It is the responsibility of the UCCS *security officer* in conjunction with the director/designate of each UCCS *designated health care component* to ensure, where session termination is not possible, either technically or from a business process perspective, automatic workstation lockout is implemented as a compensating control.
4. It is the responsibility of the UCCS *security officer* in conjunction with the director/designate of each UCCS *designated health care component* to ensure a maximum duration of inactivity prior to session termination or automatic workstation lockout is 10 minutes. The UCCS Office of Information Technology (OIT) may consider written requests for exceptions to the 10-minute requirement. These requests will be kept on file for 6 years.

Related Policies

APS 2027 Code of Conduct
APS 6002 Electronic Communications
APS 6005 IT Security Program
APS 6010 Data Governance
Reporting and filing a complaint (see Compliance and Ethics Website)
UCCS Policy 300-022 Employment Background Checks
UCCS Policy 700-001 Email as Official Means of Communication
UCCS Policy 700-006 Computer and Electronic Disposal

Reference

45 CFR § 164.310(a)(1-2)

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

Encryption and Decryption Policy
Attachment 35

Scope of Policy

This policy governs the encryption and decryption of *protected health information (PHI)* for UCCS *designated health care components*. All *workforce members* of UCCS *designated health care components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated health care components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

1. It is the Policy of UCCS and its *designated health care components* to establish and maintain this encryption and decryption policy in full compliance with all the requirements of HIPAA.
2. Responsibility for the development and implementation of this encryption and decryption policy, and any procedures associated with it, shall reside with UCCS *security officer*, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
3. Specific procedures shall be developed to specify the proper usage and application of encryption and decryption for all computers and workstations that access individually identifiable *health information*, including *PHI*.

Procedures

1. It is the responsibility of the UCCS *security officer* in conjunction with the UCCS Office of Information Technology (OIT) to implement a mechanism to encrypt and decrypt *electronic PHI (ePHI).*

2. It is the responsibility of the UCCS *security officer* in conjunction with the UCCS OIT to implement appropriate security measures, such as encryption, to protect *ePHI* from unauthorized access.
   A. Unencrypted *ePHI* will not be stored on portable electronic devices, including laptops (see Attachment 30 Workstation Use and Security Policy).

3. It is the responsibility of the UCCS *security officer* in conjunction with the UCCS OIT to, in situations where encryption is problematic, implement the alternative compensating controls below as appropriate.
   A. It is the responsibility of the UCCS *security officer* to keep an explanation for why encryption is not being implemented.
   B. Alternative, reasonable, and appropriate compensating controls if encryption is not in place for stored *ePHI*:
      1. Access controls, including unique user ID & password authentication, and user profiles.

2. Hardening of systems (see Attachment 31 Media Disposal and Re-Use and Hardware and Media Accountability Policy).
3. Physical security for access to facilities and workstations that contain or access *ePHI*, including appropriate device and media controls.
4. Technical enforcement of complex passwords where possible.
5. Enabling of system security auditing/logging, including monitoring of audit reports/ logs.
6. Correct configuration of applications to use secure protocols.
7. Implementation of automatic log-off and/or screen lock (see Attachment 34 Automatic Log-Off Policy).
8. Secure remote access.
9. Implementation of correctly configured firewalls (hardware and/or software).

Related Policies

APS 2027 Code of Conduct
APS 6002 Electronic Communications
APS 6005 IT Security Program
APS 6010 Data Governance
Reporting and filing a complaint (see Compliance and Ethics Website)
UCCS Policy 700-001 Email as Official Means of Communication

Reference

45 CFR § 164.310(a)(1-2)

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

Audit Controls Policy
Attachment 36

Scope of Policy

This policy governs audit controls for UCCS *designated health care components*. All *workforce members* of UCCS *designated health care components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated health care components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

1. It is the Policy of UCCS and its *designated health care components* to establish and maintain appropriate and effective audit controls in full compliance with the requirements of HIPAA.
2. Responsibility for the development and implementation of this audit controls policy, and any procedures associated with it, shall reside with the UCCS *security officer*, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
3. Specific procedures shall be developed to specify the proper usage and application of audit controls for all computers, workstations, and systems that access individually identifiable *health information*, including *protected health information (PHI).*

Procedures

1. It is the responsibility of the UCCS *security officer* in conjunction with the UCCS Office of Information Technology (OIT), and if necessary the director/designate of each UCCS *designated health care component*, to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use *electronic PHI (ePHI).*
2. It is the responsibility of the UCCS *security officer* in conjunction with the UCCS OIT, and if necessary the director/designate of each UCCS *designated health care component*, to establish criteria for log creation, retention, and examination of activity.
3. It is the responsibility of the UCCS *security officer* in conjunction with the UCCS OIT, and if necessary the director/designate of each UCCS *designated health care component*, to review whether new systems should be selected and to ensure that all systems have the ability to support audit requirements.
4. See Attachment 13 Information System Activity Review/Authorization and Supervision Policy/ Log-in Monitoring Policy for additional administrative practices.
5. It is the responsibility of the director/designate of each UCCS *designated health care component* to assist the UCCS *privacy officer* and the UCCS *security officer* in the event there is a for-cause audit to access audit trails and any documentation necessary.

Related Policies

APS 2027 Code of Conduct
APS 6005 IT Security Program
APS 6010 Data Governance
Reporting and filing a complaint (see Compliance and Ethics Website)

Reference

45 CFR § 164.312(b)

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

Data Integrity Controls Policy
Attachment 37

Scope of Policy

This policy governs data integrity controls for UCCS *designated health care components*. All *workforce members* of UCCS *designated health care components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated health care components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

1. It is the Policy of UCCS and its *designated health care components* to establish and maintain appropriate and effective data integrity controls in full compliance with the requirements of HIPAA.
2. Responsibility for the development and implementation of this data integrity controls policy, and any procedures associated with it, shall reside with the UCCS *security officer*, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
3. Specific procedures shall be developed to specify the proper usage and application of data integrity controls for all computers, workstations, and systems that access individually identifiable *health information*, including *protected health information (PHI)*.

Procedures

1. It is the responsibility of the UCCS *security officer* in conjunction with the UCCS Office of Information Technology (OIT), and if necessary the director/designate of each UCCS *designated health care component*, to implement policies and procedures to protect *electronic PHI (ePHI)* from improper alteration or destruction.
2. It is the responsibility of the UCCS *security officer* in conjunction with the UCCS OIT, and if necessary the director/designate of each UCCS *designated health care component*, to implement electronic mechanisms to corroborate that *ePHI* has not been altered or destroyed in an unauthorized manner.
3. It is the responsibility of the UCCS *security officer* in conjunction with the UCCS OIT, and if necessary the director/designate of each UCCS *designated health care component*, to leverage application-specific mechanisms or functionality when available to corroborate that *ePHI* has not been altered or destroyed in an unauthorized manner.
4. It is the responsibility of the UCCS *security officer* in conjunction with the UCCS OIT, and if necessary the director/designate of each UCCS *designated health care component*, to regularly review access logs for unauthorized direct access or administrator/root access to table data containing *ePHI*. The frequency at which activity logs are reviewed and the extent, frequency,

and nature of reviews are determined by the UCCS *designated health care component's* security environment and overall security management process.

5. It is the responsibility of the UCCS *security officer* in conjunction with the UCCS OIT, and if necessary each UCCS *designated health care component's* leadership, to implement the following practices as a means of protecting *ePHI* from being altered or destroyed in an unauthorized manner:
   A. Ensure appropriate physical security is in place for devices that contain or access *ePHI* (see Attachment 15 HIPAA Security Reminders Policy).
   B. Ensure HIPAA systems meet UCCS's Minimum Network Connectivity Requirements.
   C. Protect all devices against malicious software (see Attachment 16 HIPAA Malware Protection Policy).
   D. Protect sensitive data with appropriate strategies, such as secure file transfer (see Attachment 39 Data Transmission Security Policy).
   E. Implement processes to notify users and take other appropriate remedial action in the event of propagation of malicious software (see Attachment 16 HIPAA Malware Protection Policy).

Related Policies

APS 2027 Code of Conduct
APS 6002 Electronic Communications
APS 6005 IT Security Program
APS 6010 Data Governance
Reporting and filing a complaint (see Compliance and Ethics Website)
UCCS Policy 300-022 Employment Background Checks
UCCS Policy 700-001 Email as Official Means of Communication
UCCS Policy 700-006 Computer and Electronic Disposal

Reference

45 CFR § 164.312(c)(1-2)

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

Person or Entity Authentication Policy
Attachment 38

Scope of Policy

This policy governs authentication of persons or entities seeking access to *electronic protected health information (ePHI)* in the possession of UCCS *designated health care components*. All *workforce members* of UCCS *designated health care components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated health care components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

1. It is the Policy of UCCS and its *designated health care components* to establish and maintain this Policy in full compliance with all the requirements of HIPAA.
2. Responsibility for the development and implementation of this Policy, and any procedures associated with it, shall reside with each director/designate of UCCS *designated health care components*, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
3. Specific procedures shall be developed to specify the proper authentication of persons and entities who request access to individually identifiable *health information*, including *protected health information (PHI)* on UCCS computers, workstations and systems.

Procedures

1. It is the responsibility of the UCCS *security officer* in conjunction with the UCCS Office of Information Technology (OIT), and if necessary the director/designate of each UCCS *designated health care component*, to implement procedures to verify that a person or entity seeking access to *ePHI* is the one claimed.
2. It is the responsibility of the UCCS *security officer* in conjunction with the UCCS OIT, and if necessary the director/designate of each UCCS *designated health care component*, to ensure each user must be provided a unique account, with a unique user name/ID and password, for access to *ePHI* as per Attachment 32 Unique User Identification Policy.
   A. Generic or shared accounts are not permitted for access to *ePHI*.
   B. Passwords for access to *ePHI* will not be shared by UCCS employees or *workforce members*.
   C. All passwords providing access to *ePHI*, including local administrator/root passwords, must comply with UCCS Policy 700-002 Responsible Computing.
   D. Physically protect passwords.
3. It is the responsibility of the UCCS *security officer* in conjunction with the UCCS OIT, and if necessary each UCCS *designated health care component's* leadership, to review, as appropriate,

workstation, operating system, and application access logs, as well as failed or successful changes to account permissions (also see Attachment 28 Access Control and Validation Policy).

4. It is the responsibility of the UCCS *security officer* in conjunction with the UCCS OIT, and if necessary the director/designate of each UCCS *designated health care component*, to ensure systems and applications will not be configured to save passwords.
5. All of the above practices apply to vendors and third parties. A notification or suspicion of misconduct should be reported to the UCCS *privacy officer* and the UCCS *security officer* as soon as possible as per Attachment 18 HIPAA Security Incident Policy.

Related Policies

APS 2027 Code of Conduct
APS 6005 IT Security Program
APS 6010 Data Governance
Reporting and filing a complaint (see Compliance and Ethics Website)
UCCS Policy 300-022 Employment Background Checks
UCCS Policy 700-006 Computer and Electronic Disposal

Reference

45 CFR § 164.312(d)

University of Colorado Colorado Springs

Effective Date: _____
Last Revised: _____

Data Transmission Security Policy
Attachment 39

Scope of Policy

This policy governs data transmission security for UCCS *designated health care components*. All *workforce members* of UCCS *designated health care components* must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Those officers, agents, employees, *business associates*, contractors, affected vendors, temporary workers, students, and volunteers associated with UCCS *designated health care components* must read, understand, and comply with this policy in full and at all times.

Policy Statement

1. It is the Policy of UCCS and its *designated health care components* to establish and implement technical security measures to guard against unauthorized access to *electronic protected health information (ePHI)* that is being transmitted over an electronic communications network, in full compliance with the requirements of HIPAA.
2. Responsibility for the development and implementation of these procedures shall reside with the UCCS *security officer*, who shall ensure that these procedures are maintained, updated as necessary, and implemented fully throughout our organization.
3. Specific data transmission security procedures shall be developed to protect individually identifiable *health information*, including *ePHI*.

Procedures

1. It is the responsibility of the UCCS *security officer* in conjunction with the UCCS Office of Information Technology (OIT), and if necessary the director/designate of each UCCS *designated health care component*, to implement technical security measures to guard against unauthorized access to *ePHI* that is being transmitted over an electronic communications network.
2. It is the responsibility of the UCCS *security officer* in conjunction with the UCCS OIT, and if necessary the director/designate of each UCCS *designated health care component*, to implement security measures to ensure that electronically transmitted *ePHI* is not improperly modified without detection, until disposed.
3. It is the responsibility of the UCCS *security officer* in conjunction with the UCCS OIT, and if necessary the director/designate of each UCCS *designated health care component*, to ensure wired and wireless transmission of *ePHI* will use secure protocols.
4. It is the responsibility of the UCCS *security officer* in conjunction with the UCCS OIT, and if necessary the director/designate of each UCCS *designated health care component*, to ensure all remote access of *ePHI* must be by secure methods only.

5. It is the responsibility of the UCCS *security officer* in conjunction with the UCCS OIT, and if necessary the director/designate of each UCCS *designated health care component*, to ensure unprotected *ePHI* shall not be sent via unencrypted methods.
   A. It is acceptable to send *ePHI* via email in encrypted, password-protected attachments to known business partners, and in response to legitimate requests if no secure channelexists.
6. UCCS *workforce members* must delete or redact *ePHI* from the body of received email before replying to it.
7. It is the responsibility of the UCCS *security officer* in conjunction with the UCCS OIT, and if necessary the director/designate of each UCCS *designated health care component*, to implement a mechanism to encrypt *ePHI* whenever deemed appropriate.

Related Policies

APS 2027 Code of Conduct
APS 6002 Electronic Communications
APS 6005 IT Security Program
APS 6010 Data Governance
Reporting and filing a complaint (see Compliance and Ethics Website)
UCCS Policy 700-001 E-Mail as Official Means of Communication
UCCS Policy 700-006 Computer and Electronic Disposal

Reference

45 CFR § 164.312(e)(1)

UCCS HealthCircle

UNIVERSITY OF COLORADO
COLORADO SPRINGS

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("BA Agreement") is part of an agreement dated_____by and between The Regents of the University of Colorado, a body corporate, for and on behalf of the University of Colorado Colorado Springs ("University" or "Covered Entity") and _____, a ("Business Associate"), who has a relationship with University, but only to the extent such subsidiary creates, receives, maintains, or transmits Protected Health Information (as defined below) for or on behalf of University through the performance of services to University. The purpose of this BA Agreement is to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) including all pertinent regulations (45 CFR Parts 160 and 164 referred to herein as the "HIPAA Security Rule" and the "HIPAA Privacy Rule") issued by the U.S. Department of Health and Human Services as either have been amended by Subtitle D of the Health Information Technology for Economic and Clinical Health Act (the "HITECH" Act), as Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5). Covered Entity and Business Associate are collectively referred to as "Parties" in this Agreement and may be referred to individually as a "Party."

RECITALS

A. Covered Entity is a covered entity that is a hybrid entity as such terms are defined under HIPAA and as such is required to comply with the requirements thereof regarding the confidentiality, security and privacy of Protected Health Information.
B. Business Associate has entered into one or more agreement(s) with Covered Entity ("the Services Agreement") pursuant to which Business Associate will provide services that involve the use and/or disclosure of Protected Health Information for or on behalf of Covered Entity and must comply with privacy and security requirements imposed upon Business Associate by HIPAA and the HITECH Act and any regulations promulgated thereunder.
C. The health care component of the Covered Entity, to which HIPAA and HITECH requirements apply, is the UCCS Health Circle Clinics.

NOW THEREFORE, in consideration of the mutual covenants, promises and agreements contained in the Services Agreement and this BA Agreement, the Parties agree as follows:

1. Definitions.

Terms used, but not otherwise defined, in this BA Agreement shall have the same meaning as those terms have under the HIPAA Security Rule and the

HIPAA Privacy Rule and in the HITECH Act and in any subsequent creation or modification of applicable rules.

For purposes of this BA Agreement, the following terms shall have the meanings ascribed to them below:

A. "**Administrative Safeguards"** shall mean administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect ePHI and to manage the conduct of the Business Associate's workforce in relation to the protection of that information.
B. **"Breach"** as defined in 45 CFR §164.402, is the acquisition, access, use, or disclosure of PHI that is not permitted by the HIPAA Privacy Rule and which compromises the security or privacy of the PHI. The acquisition, access, use or disclosure of PHI in a manner not permitted by the HIPAA Privacy Rule is presumed to be a breach unless a risk assessment, which will include the factors in 45 CFR §164.402(2), demonstrates that there is a low probability that the PHI has been compromised.
C. "Days" means calendar days unless "business days" is specified.
D. **"Designated Record Set"** shall have the meaning specified under the HIPAA Privacy Rule, including, but not limited to, 45 CFR §164.501.
E. **"Electronic Protected Health Information" or "ePHI"** shall have the meaning found in 45 CFR §160.103 which is PHI that is transmitted or maintained in electronic media.
F. **"Individual"** means the person who is the subject of Protected Health Information and shall include a person who qualifies as a personal representative in accordance with 45 CFR §164.502(g).
G. **"Information"** shall mean any health information, including individually identifiable health information, as defined in 45 CFR §160.103.
H. **"Limited Data Set"** shall mean PHI that excludes the direct identifiers of the Individual or of relatives, employers or household members of the Individual as described in 45 CFR § 164.514(e)(2).
I. **"Physical Safeguards"** shall mean physical measures, policies, and procedures to protect a Party's electronic information systems and related buildings and equipment, from natural and environmental hazards and unauthorized intrusions.
J. **"Protected Health Information" or "PHI"** shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 CFR §160.103, as applied to the information created or received by Business Associate from or on behalf of the UCCS Health Circle Clinics.
K. **"Required By Law"** shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 CFR §164.103.
L. **"Secretary"** shall mean the Secretary of the Department of Health and Human Services or his or her designee.
M. **"Security"** shall mean all of the Administrative, Physical, and Technical Safeguards in or for an information system.

N. **"Security Incident"** means the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system.
O. **"Technical Safeguards"** means the technology and the policy and procedures for its use that protect ePHI and control access to it.
P. **"Unsecured PHI"** is PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals via the methods or technologies established by the Department of Health and Human Services to secure PHI.
Q. **"UCCS Health Circle Clinics"** includes the following health care clinics owned and operated by the University: Primary Care Clinic, Veteran's Health and Trauma Clinic, Center for Active Living, Peak Nutrition Clinic, and UCCS Aging Center.

2. <u>Permitted Uses and Disclosures of PHI by Business Associate.</u>

Except as otherwise expressly limited in this BA Agreement, Business Associate may, in its capacity as a business associate to the Covered Entity:
A. Use or disclose PHI to perform functions, activities or services for, or on behalf of, Covered Entity under the Services Agreement(s);
B. Use PHI for the proper management and administration of Business Associate or to carry out the present and future legal responsibilities of Business Associate;
C. Disclose PHI for the proper management and administration of Business Associate or to carry out the present and future legal responsibilities of Business Associate if the disclosure is Required By Law, or if Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware that the confidentiality of the information was breached;
D. Provide Data Aggregation services to Covered Entity as permitted by 45 CFR §164.504(e)(2)(i)(B); and
E. De-identify any and all PHI in accordance with 45 C.F.R. § 164.514(b). Covered Entity acknowledges and agrees that de-identified information is not PHI and that Business Associate may use such de-identified information for any lawful purpose.

3. <u>Obligations of Business Associate.</u>

Business Associate includes its directors, officers, subcontractors, employees, affiliates, agents, and representatives.

A. **Uses and Disclosures.** Business Associate agrees not to use or disclose PHI other than as permitted or required by the Services Agreement, this BA Agreement or as Required By Law.

B. **Appropriate Safeguards.** Business Associate agrees to use appropriate Administrative, Physical and Technical Safeguards to protect the confidentiality, integrity and availability of the Covered Entity's PHI that it creates, receives, maintains, or transmits on behalf of the Covered Entity and to prevent the use, disclosure or access of the PHI, other than as provided for by the Services Agreement or this BA Agreement. For ePHI, appropriate safeguards mean all the safeguards of the HIPAA Security Rule and shall include technologies and methodologies prescribed by the Secretary of the Department of Health and Human Services in regulations implementing the HITECH Act. Business Associate agrees to verify that it has implemented such safeguards and that it complies with all standards and implementation specifications set out in the privacy and security regulations.

C. Reporting of Improper Uses or Disclosures, Security Incidents and Breaches.

1) **Improper Use or Disclosure.** Business Associate agrees to report to the Privacy Officer of the Covered Entity any use or disclosure of PHI or ePHI not provided for by the Agreement and this BA Agreement within five (5) days of becoming aware of such use or disclosure. A written report will be provided to the CE's Privacy Officer no later than ten (10) days from the date Business Associate becomes aware of the improper use or disclosure.
2) **Security Incident.** Business Associate agrees to report to the CE's Privacy Officer any successful security incident within ten (10) days of becoming aware of such incident, regardless of whether the incident constitutes a Breach as defined in 45 CFR §164.202. This Agreement serves as Business Associate's notice to Covered Entity that attempted but unsuccessful Security Incidents regularly occur and that no further notice will be made by Business Associate unless there has been a successful Security Incident or attempts or patterns of attempts that Business Associate reasonably determines to be suspicious.
3) **Breaches.** In the event of a Breach of Unsecured PHI that Business Associate accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds or uses on behalf of Covered Entity, Business Associate agrees to report such Breach to Covered Entity immediately, but in no event more than ten (10) days after discovering the Breach. A Breach shall be treated as discovered at the point when any member of the Business Associate's workforce, contractors, agents or officials is aware, or would be aware by exercising reasonable diligence, of the Breach. A written report must be provided to the Privacy Officer no later than five (5) days from the date Business Associate becomes aware of the Breach. Notice of a Breach shall be in writing and shall include, at a minimum, to the extent known at the time of the notice: (a) the identification of each individual whose PHI has been, or is reasonably believed to have been, accessed, acquired, or disclosed during the Breach; (b) a description of what happened, including the date of the Breach and the date of discovery of the Breach; (c) a description of the

types of PHI that were involved in the Breach; (d) the identity of who made the non-permitted access, use or disclosure and who received the non-permitted access, use or disclosure, (e) a description of the Business Associate's investigation and response to the Breach, (f) actions taken to prevent any further non-permitted access, uses or disclosures, and (g) actions taken to mitigate any deleterious effect of the non-permitted access, use or disclosure. Business Associate shall provide additional information to the Covered Entity as reasonably requested.

4) **Mitigation.** Business Associate shall mitigate, to the extent practicable, any harmful effect from a use or disclosure of PHI in violation of the requirements of the Services Agreement or this BA Agreement or from a Breach of Unsecured PHI.

D. **Minimum Necessary.** Business Associate, its agents or subcontractors agree only to use and to disclose the minimum amount of PHI necessary to accomplish the purpose of the use or disclosure in accordance with the Minimum Necessary requirements of the HIPAA Privacy Rule including, but not limited to 45 C.F.R. §§164.502(b) and 164.514(d).

E. **Access to and Amendment of PHI.** Business Associate shall make PHI maintained by Business Associate in Designated Record Sets available to CE for inspection and copying within five (5) business days of a request by CE to enable CE to fulfill its obligations to permit individual access to PHI under the Privacy Rule, including, but not limited to, 45 CFR Section 164.524. Within five (5) business days of receipt of a request from CE for an amendment of PHI or a record about an Individual contained in a Designated Record Set, Business Associate shall make such PHI available to CE for amendment and/or incorporate any such amendment to enable CE to fulfill its obligations with respect to requests by Individuals to amend their PHI under the HIPAA Privacy Rule, including, but not limited to, 45 CFR Section 164.526. If any Individual requests an amendment of PHI directly from Business Associate, Business Associate must notify CE in writing within five (5) days of receipt of the request and make such amendments to the extent required by the HIPAA Privacy Rule. Covered Entity shall be responsible for responding to such requests in accordance with the HIPAA Privacy Rule.

F. **Accounting and Documentation of Disclosures.** Business Associate agrees to document disclosures of PHI and information as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures in accordance with 45 CFR §164.528 and the HITECH Act, as applicable. At a minimum, such documentation shall include: (i) the date of the disclosure; (ii) the name of the entity or person who received PHI and, if known, the address of the entity or person; (iii) a brief description of the PHI disclosed; and (iv) a brief statement of the purpose of the disclosure that reasonably informs the Individual of the basis for the disclosure. This documentation will be retained for a period of six (6) years following the disclosure unless it is transferred to the Covered Entity at the termination of the Agreement. Within ten (10) business days after a written request by Covered Entity, Business Associate agrees to provide such documentation to

Covered Entity to respond to request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR §164.528. In the event that an Individual requests an accounting directly to Business Associate, Business Associate shall forward such request to Covered Entity in writing within five (5) days of receipt of such request. It shall be Covered Entity's responsibility to prepare and deliver any such accounting to the Individual.

G. **Use or Disclosure Restrictions and Confidential Communications.** Business Associate will not respond directly to an Individual's requests to restrict the use or disclosure of PHI or to send all communication of PHI to an alternate address. Business Associate will refer such requests to the CE so that the CE can coordinate and prepare a timely response to the requesting Individual and provide direction to Business Associate.

H. **Audits, Inspection, and Enforcement.** Upon receipt of a written request by CE, Business Associate and its agents or subcontractors shall allow CE and its authorized agents or contractors to conduct a reasonable inspection of the facilities, systems, books, records, agreements, policies, procedures, and practices relating to the use or disclosure of PHI pursuant to this BA Agreement for the purpose of determining whether Business Associate has complied with this BA Agreement; provided, however, that: (i) Business Associate and CE shall mutually agree in advance upon the scope, timing and location of such an inspection; (ii) CE, and its authorized agents or contractors, shall protect the confidentiality of all confidential and proprietary information of Business Associate to which CE has access during the course of such inspection; and (iii) CE and its authorized agents or contractors shall execute a nondisclosure agreement, upon terms mutually agreed upon by the parties, if requested by Business Associate. It is understood that the examination by CE and its authorized agents or contractors may include such examination as is necessary for Business Associate and such agents or contractors to certify to CE that extent to which Business Associate's Administrative, Physical and Technical Safeguards comply with HIPAA, the HIPAA regulations and this BA Agreement. The fact that CE inspects, or fails to inspect, or has the right to inspect, Business Associate's facilities, systems, books, records, agreements, policies, procedures, and practices does not relieve Business Associate of its responsibility to comply with this BA Agreement, nor does CE's (i) failure to detect or (ii) detection, but failure to notify Business Associate or require Business Associate's remediation of any unsatisfactory policies, procedures and practices, constitute acceptance of such practice or a waiver of CE's enforcement rights under the Agreement.

I. **Governmental Access to Records.** Business Associate agrees to make internal practices, books, and records, including policies and procedures, relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of Covered Entity available to the Secretary, in a time and manner reasonably designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with HIPAA and the HITECH Act.

J. **Training.** Business Associate agrees to provide adequate training to its employees and subcontractors to ensure compliance with HIPAA and the HITECH Act.
K. **Marketing.** Business Associate shall use and disclose PHI for marketing purposes only as approved by the Covered Entity, and in accordance with §13406(a) of the HITECH Act.
L. **Sale of PHI.** Business Associate acknowledges that it has no ownership rights with respect to the PHI and is prohibited from selling PHI.
M. **Business Associate's Agents.** If Business Associate uses one or more subcontractors or agents to provide services under the Agreement, and such subcontractors or agents receive or have access to PHI, each subcontractor or agent shall sign a Business Associate Agreement with Business Associate containing substantially the same provisions as this BA Agreement, agreeing to comply with the obligations of Business Associate described in this BA Agreement with respect to the PHI maintained by it. Business Associate shall, in its reasonable discretion, implement and maintain sanctions against agents and subcontractors that violate such restrictions and conditions and shall mitigate the effects of any such violation.

4. Compliance with HIPAA Privacy and Security Rules.

Business Associate acknowledges that, to the extent that it performs functions, activities, or services for the Covered Entity that involve the use or disclosure of PHI, it has a statutory duty under the HITECH Act to, among other duties, use and disclose PHI only in compliance with 45 CFR §164.504(e) (the provisions of which have been incorporated into the Agreement), 45 CFR §164.308 (Security Standards), 45 CFR §164.310 (Administrative Safeguards), 45 CFR §164.312 (Technical Safeguards), and 45 CFR §164.316 (Policies and Procedures and Documentation Requirements), as amended from time to time.

5. Obligations of Covered Entity.

Covered Entity agrees that Covered Entity, its directors, officers, subcontractors, employees, affiliates, agents, and representatives shall:

A. Be responsible for using appropriate Administrative, Physical, and Technical Safeguards to maintain and ensure the confidentiality, privacy and security of PHI transmitted to Business Associate pursuant to this Agreement, in accordance with the standards and requirements of the HIPAA Privacy Rule, until such PHI is received by Business Associate;
B. Not require Business Associate to use or to disclose PHI in any manner that would violate applicable Federal and State laws if such use or disclosure were done by Covered Entity;
C. Require Business Associate to disclose PHI directly to another party only for the purposes allowed by the Privacy Rule; and

D. Ensure that its notice of privacy practices permits Covered Entity to use and disclose PHI in the manner that Business Associate is authorized to use and disclose PHI under the BA Agreement and the Services Agreement;
E. Obtain any consent, authorization or permission that may be required by the HIPAA Privacy Rule or any other applicable federal, state or local laws and/or regulations prior to furnishing Business Associate the Protected Health Information pertaining to an individual for the Business Associate's use and/or disclosure as authorized under the BA Agreement and the Services Agreement;
F. Not furnish Business Associate Protected Health Information that is subject to any arrangement permitted or required of Covered Entity, including but not limited to, an arrangement agreed to by Covered Entity under 45 CFR §164.522 that restricts the use and/or disclosure of Protected Health Information by the Business Associate as otherwise authorized under this BA Agreement and the Service Agreement(s); and
G. Provide Business Associate with any changes in, or revocation of, permission to use or disclose PHI to the extent it may affect Business Associate's permitted or required uses or disclosures.

6. Term.

The term of this BA Agreement shall be concurrent with the term of the Services Agreement(s).

7. Termination.

A. **Material Breach**. In addition to any other provisions in the Services Agreement regarding breach, a breach by either Party of any provision of this BA Agreement, as reasonably determined by the other Party, shall constitute a material breach of the Services Agreement and shall provide grounds for termination of the Services Agreement by the non-breaching Party pursuant to the provisions of the Services Agreement covering termination for default.
B. **Reasonable Steps to Cure Breach**. If either Party knows of a pattern of activity or practice of the other Party that constitutes a material breach or violation of such Party's obligations under the provisions of this BA Agreement and does not terminate the Services Agreement pursuant to Section 7.A., then the non-breaching Party shall take reasonable steps to cure such breach or end such violation, as applicable. If the non-breaching Party's efforts to cure such breach or end such violation are unsuccessful, such Party shall either (i) terminate the Services Agreement, if feasible or (ii) if termination of the Services Agreement is not feasible, such Party may report the breach or violation to the Secretary.
C. **Judicial or Administrative Proceedings**. Either Party may terminate the Agreement, effective immediately, if (i) the other Party is found guilty or pleads nolo contendere in a criminal proceeding for a violation of HIPAA, the HIPAA regulations or other security or privacy laws or (ii) a finding or

stipulation that the other Party has violated any standard or requirement of HIPAA, the HIPAA regulations or other security or privacy laws is made in any administrative or civil proceeding in which the Party has been joined.

D. **Effect of Termination**.

1) Except as provided in paragraph 2) of this subsection 7(D), upon termination of this BA Agreement for any reason, Business Associate shall return or destroy all PHI that Business Associate or its agents or subcontractors still maintain in any form and shall retain no copies of such PHI. If Business Associate elects to destroy the PHI, Business Associate shall certify in writing to CE that such PHI has been destroyed.
2) If Business Associate believes that returning or destroying the PHI is not feasible, Business Associate shall promptly provide CE notice of the conditions making return or destruction infeasible. In such event, Business Associate shall continue to extend the protections of this BA Agreement to such PHI and shall limit further use of such PHI to those purposes that make the return or destruction of such PHI infeasible.

8. Injunctive Relief.

Subject to Section 9, either party shall have the right to seek injunctive and other equitable and legal relief against the other party or any of its subcontractors or agents in the event of any use or disclosure of PHI in violation of the Services Agreement, this BA Agreement or applicable law.

9. No Waiver of Immunity.

No term or condition of this BA Agreement shall be construed or interpreted as a waiver, express or implied, of any of the immunities, rights, benefits, protection, or other provisions of the Colorado Governmental Immunity Act, CRS 24-10-101 *et seq.* or the Federal Tort Claims Act, 28 U.S.C. 2671 *et seq.* as applicable, as now in effect or hereafter amended.

10. Limitation of Liability and Insurance.

Notwithstanding any provision in the Services Agreement to the contrary, BA's indemnification obligations under Section 12 of this Agreement shall not be subject to any limitations on cumulative liability or based on classification of damages awarded in any matter for which CE is indemnified. In addition to any insurance requirements in the Agreement, Business Associate shall maintain appropriate insurance to cover loss of PHI data and claims based upon alleged violations of privacy rights through improper use or disclosure of PHI.

11. Disclaimer.

CE makes no warranty or representation that compliance by Business Associate with this Agreement, HIPAA or the HIPAA regulations will be adequate or

satisfactory for Business Associate's own purposes. Business Associate is solely responsible for all decisions made by Business Associate regarding the safeguarding of PHI.

12. <u>Indemnification</u>.

In the event of any unauthorized use or disclosure of PHI constituting a "Breach" as defined under 45 C.F.R. § 164.402 which is caused by the negligent act(s) or omission(s) of Business Associate, Business Associate agrees to indemnify CE, to the extent Business Associate is responsible, from and against (i) any administrative fines or penalties assessed against CE by the Secretary or other regulatory authority having jurisdiction; (ii) any award which may be made pursuant to a state attorney general action and levied against CE; and (iii) in the event that any such Breach requires the issuance of notice(s) to affected individuals pursuant to the relevant provisions of the HITECH Act, all direct reasonable costs associated with production and delivery of such required notice(s). The indemnification obligations under this section are subject to CE's (a) making written demand for Indemnification from Business Associate pursuant to the foregoing; (b) to the extent CE has notice of same, promptly notifying Business Associate of any investigation or the filing of any action by the Secretary, any state attorney general, or other regulatory authority having jurisdiction; (c) granting to Business Associate the right to determine the means and methods by which any required notices are delivered to affected individuals, and (d) granting to Business Associate sole right to control any associated defense or negotiation for settlement or compromise. Business Associate agrees to work cooperatively with CE to ensure that liability is properly determined and assigned by the Secretary or other regulatory authority having jurisdiction with regard to any such Breach.

13. <u>Miscellaneous.</u>

A. **Regulatory References.** A reference in this BA Agreement to a section in the HIPAA Privacy Rule, the HIPAA Security Rule, or the HITECH Act and any regulations thereunder means the section as in effect or as amended, and for which compliance is required.
B. **Amendment to Comply with Law.** The Parties acknowledge that state and federal laws relating to data security and privacy are rapidly evolving and that amendment of this BA Agreement may be required to provide for procedures to ensure compliance with such developments. Unless either Party should terminate this BA Agreement and the Services Agreement as described below, the Parties specifically agree to take such action, as is necessary to implement the standards and requirements of the HIPAA Privacy Rule, the HIPAA Security Rule, other standards and requirements of HIPAA, the HITECH Act and other applicable laws relating to the security or privacy of PHI. The Parties understand and agree that CE may be required to obtain satisfactory written assurance from Business Associate that Business

Associate will adequately safeguard all PHI. Upon the request of either Party, the other Party agrees to enter promptly into negotiations concerning the terms of an amendment to this BA Agreement embodying written assurances consistent with the standards and requirements of the HIPAA Privacy Rule, the HIPAA Security Rule, other standards and requirements of HIPAA, the HITECH Act and other applicable laws relating to the security or privacy of PHI. Either Party may terminate this BA Agreement and the Services Agreement upon thirty (30) days written notice in the event (i) the other Party does not promptly enter into negotiations to amend this BA Agreement when requested pursuant to this Section or (ii) the other Party does not enter into an amendment to this BA Agreement providing assurances regarding the safeguarding of PHI that the requesting Party, in its reasonable discretion, deems sufficient to satisfy the HIPAA Privacy Rule, the HIPAA Security Rule, other standards and requirements of HIPAA, the HITECH Act and other applicable laws relating to the security or privacy of PHI. A waiver with respect to one event shall not be construed as continuing, or as a bar to or waiver of any right or remedy as to subsequent events.

C. **Assistance in Litigation or Administrative Proceedings**. Business Associate shall make itself, and any subcontractors, employees or agents assisting Business Associate in the performance of its obligations under the Agreement, available to CE, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against CE, its directors, officers or employees based upon a claimed violation of the HIPAA Privacy Rule, the HIPAA Security Rule, other standards and requirements of HIPAA, the HITECH Act and other applicable laws relating to the security or privacy of PHI, except where Business Associate or its subcontractor, employee or agent is a named adverse party. Subject to Section 12 herein, If the claimed violation relates to or is in connection with Business Associate's use or disclosure of PHI or its performance of functions, activities, or services for or on behalf of the Covered Entity under the Services Agreement, such assistance in litigation or administrative proceedings shall be provided at no cost to the CE.

D. **Interpretation.** The provisions of this BA Agreement, as amended, shall prevail over any provisions in the Services Agreement that may conflict or appear inconsistent with any provision in this BA Agreement. Any ambiguity in this BA Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with the HIPAA Privacy Rule, the HIPAA Security Rule, other standards and requirements of HIPAA, the HITECH Act and other applicable laws relating to the security or privacy of PHI. If the provisions differ but are permitted by HIPAA or the HITECH Act, the provisions of this BA Agreement shall control.

E. **Survival.** The obligations of Business Associate under Sections 2, 3, 4, 7.D, and 12 of this BA Agreement shall survive the termination of the Agreement and this BA Agreement.

F. **No Third-Party Beneficiaries.** Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other

than Covered Entity, Business Associate and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

14. <u>Representatives and Notice</u>.

A. **Representatives.** For the purposes of the Agreement, the individuals identified elsewhere in the Agreement shall be the representatives of the respective Parties. If no representatives are identified in the Agreement, the individuals listed below are hereby designated as the Parties' respective representatives for purposes of this BA Agreement. Either Party may from time to time designate in writing new or substitute representatives.

B. **Notices**. All required notices shall be in writing and shall be deemed sufficient if delivered as provided in the Agreement to the representatives of the Parties at the addresses set forth below.

University/Covered Entity Representative:

Title: Director of Campus Compliance / Privacy Officer

Phone: 719-255-3837

Address: 1420 Austin Bluffs Parkway
Colorado Springs, CO 80918

With a copy to: Office of University Counsel
1420 Austin Bluffs Parkway
Colorado Springs, CO 809189

Company Representative:

Name: _____

Title: _____

Department: _____

Address: _____

_____

SIGNATURES REQUIRED ON THE FOLLOWING PAGE

IN WITNESS WHEREOF, the Parties hereto have duly executed this BA Agreement as of the dates set forth below.

THE REGENTS OF THE UNIVERSITY OF COLORADO	**BUSINESS ASSOCIATE**
By: _____	**By:** _____
Print Name: _____	**Print Name:** _____
Title: _____	**Title:** _____
Date: _____	**Date:** _____

Attest (Seal)

By: _____
Corporate Secretary or Equivalent

University of Colorado Colorado Springs

Patient Name(s) _____

Medical Record # _____

Date of Birth _____

Contact Phone # _____

AUTHORIZATION TO RELEASE AND/OR OBTAIN PATIENT INFORMATION

☐ Obtain From: (Releasing facility)

Please check a HealthCircle Clinic or complete provider contact details in the space provided.

☐ Aging Center (719) 255-8002 (719) 255- 8006 Fax	☐ Center for Active Living (719) 255- 8067 (719) 255- 8044 Fax
☐ Peak Nutrition Clinic (719) 255- 7524 (719) 255- 8044 Fax	☐ Nurse-Family Partnership© (719) 255-8049
☐ Veterans Health & Trauma (719) 255- 8003 (719) 255- 8075 Fax	☐ Primary Care Clinic (719) 255- 8001 (719) 255- 8044 Fax

Provider Name: _____

_____

Address: _____

City, State, Zip: _____

Phone: _____ Fax: _____

Purpose:

- ☐ Continuity of Care
- ☐ Personal Use
- ☐ Legal
- ☐ Coordination of Care
- ☐ Other _____

INFORMATION TO BE OBTAINED (check all that apply):

Date of Service Range (month/year):

FROM: / TO: /

- ☐ Discharge Summary
- ☐ History & Physical
- ☐ Clinic Progress Notes
- ☐ Mental Health Treatment

☐ Release To: (Receiving facility)

Please check a HealthCircle Clinic or complete provider contact details in the space provided.

☐ Aging Center (719) 255-8002 (719) 255- 8006 Fax	☐ Center for Active Living (719) 255- 8067 (719) 255- 8044 Fax
☐ Peak Nutrition Clinic (719) 255- 7524 (719) 255- 8044 Fax	☐ Nurse-Family Partnership© (719) 255-8049
☐ Veterans Health & Trauma (719) 255- 8003 (719) 255- 8075 Fax	☐ Primary Care Clinic (719) 255- 8001 (719) 255- 8044 Fax

Provider Name: _____

_____

Address: _____

City, State, Zip: _____

Phone: _____ Fax: _____

Purpose:

- ☐ Continuity of Care
- ☐ Personal Use
- ☐ Legal
- ☐ Coordination of Care
- ☐ Other _____

INFORMATION TO BE RELEASED (check all that apply):

Date of Service Range (month/year):

FROM: / TO: /

- ☐ Drug/Alcohol Treatment
- ☐ Laboratory Reports
- ☐ Radiology Images
- ☐ Other:

Discharge Summary	Drug/Alcohol
History & Physical	Treatment
Clinic Progress Notes	Laboratory
Mental Health Treatment	Reports
	Radiology
	Images Other:

AUTHORIZATION: I hereby give the releasing facility permission to disclose my individually identifiable health information as listed above. I understand that once this information is disclosed, it may no longer be protected. I understand this authorization is voluntary, and further treatment cannot be conditioned upon my signing this authorization. I acknowledge that incomplete forms cannot be processed and **THERE MAY BE A COST TO COPY THE RECORDS OR WRITE A TREATMENT SUMMARY.**

I understand there are limited exceptions to these provisions in the Colorado Statutes. These require reporting of threats of violence, harm, or child or elder abuse and neglect (from either evidence or suspicion), or when subpoenaed by the courts, to proper authorities. Certain other exceptions exist and will be explained as necessary.

I understand that **this consent expires the sooner of one year from the date of my signature or 6 months from the last appointment** unless otherwise specified as follows: _____ I understand I can take back permission to release my medical records at any time, except to the extent that action has already been taken to comply with it. I understand I must provide notice in writing if I choose to revoke this authorization before the date/event of expiration, and that the written revocation must be signed and dated with a date that is later than the date of this authorization. A copy, fax, or scan of this form is to be considered as valid as the original.

_____ _____

Signature of Patient or Authorized Representative **Date of Signature**

_____ _____

Printed Name **Relationship to Patient (if applicable)**

(Please Provide a Copy of This Form to the Patient)

Revocation of Authorization to Release Information

I hereby revoke my authorization to use/disclose information indicated above:

_____ _____

Signature of Patient or Personal Representative Date

University of Colorado Colorado Springs

Patient Name(s)
Medical Record #
Date of Birth
Contact Phone #

HIPAA Authorization for Release of Health Information – Media

I hereby authorize University of Colorado Colorado Springs (UCCS) Covered Entities to use and disclose information about me for the purposes of creating press releases, news stories, photographs or video clips, website and/or publications, as well as stand-alone pictures/graphics in which I may appear and/or be heard, for use in internal UCCS publications and/or disclosure to external (non-UCCS) media.

The information about me may include my: name, treatment modality, age, duration of treatment, treatment plan, diagnoses, city and state of residence, photographs, location of UCCS treating facility and information about my life and how I came to UCCS or my on-going treatment. The information may also be disclosed to external media in the form of press releases, stories, photographs or video clips. It may also be used for internal purposes or on the UCCS website or through UCCS's own marketing or educational campaigns. UCCS will not receive any direct or indirect payment from or on behalf of any third party in exchange for the release of this information about me.

I understand the provision of health care treatment, payment for my health care and my health care benefits are not dependent on this authorization. I understand I am not required to sign this authorization. The information will not be used or disclosed without authorization. I understand any information used or disclosed pursuant to this authorization may be subject to redisclosure.

I understand I have the right to revoke this authorization in writing, except to the extent information has already been released pursuant to this authorization at the time of the revocation. I can revoke this authorization by sending correspondence to the UCCS Director of Campus Compliance / Privacy Officer, 1420 Austin Bluffs Parkway Colorado Spring CO 80918.

I hereby release, discharge and agree to hold UCCS harmless from any liability that may arise from the release of information authorized above.

This authorization shall expire 10 years from date of signature.

_____ _____

Signature of Patient or Authorized Representative **Date of Signature**

_____ _____

Printed Name **Relationship to Patient (if applicable)**

If the patient is a minor or has a personal representative, I represent that I am the legal parent/guardian/personal representative of the Patient named above and I am not prohibited by Court Order from releasing access to the requested information.

University of Colorado Colorado Springs

Patient Consent and Release Agreement

I, the undersigned, grant to University of Colorado Colorado Springs (UCCS) perpetual right and license to use, reproduce, print, publish, broadcast and rebroadcast, as well as to copyright, my testimonial statement, voice, picture, name and likeness in any and all media and types of advertising and promotion (collectively referred to as "Advertising") for the UCCS and their products and services.

All right, title, and interest in and to my name, testimonial statement, voice, picture, and likeness used in Advertising pursuant to this Consent and Release, including all copyrights therein, will be the sole property of the UCCS, free from any claims whatsoever by me or my employer.

I understand that I will not have any right to compensation in connection with the UCCS use of my name, testimonial statement, voice, picture, or likeness. I hereby release UCCS and their successors and assigns from any and all claims arising out of their use of my name, testimonial statement, voice, picture, and likeness as agreed to in this Consent and Release, including without limitation any claims based on libel, slander, or the rights of publicity, privacy or personality. I hereby waive any right to review any Advertising and agree that no advertisement or other material need be submitted to me for any further approval.

I acknowledge that this permission authorizes UCCS to post my testimonial statement, voice, picture, name, and likeness on third party social media web sites (including Facebook, Twitter, Instagram, and YouTube), which may require UCCS to grant the owners and users of such sites a broad license to use such materials for any purpose without notice to or approval from me.

The statements attributed to me in any testimonial I provide reflect my actual experience with UCCS and my honest opinions about UCCS Covered Entities and/or their products and services. I understand that I have the right to revoke this authorization in writing, by sending correspondence to the UCCS Director of Campus Compliance / Privacy Officer, 1420 Austin Bluffs Parkway Colorado Spring CO 80918. If I revoke this authorization, it will not impose any obligation upon UCCS to recall or destroy any materials already used, published or disclosed.

This Consent and Release does not in any way conflict with any existing commitment on my part. I am of the age of 18 or older and have the right to contract in my own name and, if applicable, on behalf of my employer with respect to this Consent and Release. I understand that the provision of health care treatment, payment for my health care, and my health care benefits are not dependent upon this Consent and Release.

I understand that this Consent and Release does not obligate UCCS to make any use of any of the rights granted herein.

_____ _____

Signature of Releasor or Authorized Representative **Date of Signature**

_____ _____

Printed Name **Relationship to Patient (if applicable)**

University of Colorado Colorado Springs

Authorization (Permission) to Use or Disclose (Release) Identifiable Health Information for Research

Please type your response in the gray-box area. The box will expand to accommodate your full text.

1. **Participant's Name:**

2. **Date of Birth:**

3. **Title of Protocol:**

4. **Name of Principal Investigator:**

5. **What is the Purpose of This Form?**
   You are being considered for participation in **[Research Protocol Title].** Researchers would like to use your protected health information which includes your paper or electronic medical record for this research study. This information may include data that identifies you. Please carefully review the information below. If you agree that researchers can use your personal health information, you must sign and date this form to give them your permission. If you do not sign this permission form, you will not be able to take part in this research study.

6. **What personal health information do the researchers want to use?**
   The researchers want to copy and use portions of your medical record that they will need for their research. If you enter the research study, information that will be used and/or released may include the following information that your researcher has checked:

   - ☐ Name, address, phone number, age, sex, ethnicity.
   - ☐ The history and diagnosis of your disease;
   - ☐ Specific information about the treatments you received, including previous treatment(s) you may have had;
   - ☐ Information about other medical conditions that may affect your treatment;
   - ☐ Medical data may include laboratory test results, tumor and heart measurements, x-rays, CT scans, photographs of radiation therapy target areas, and pathology results;
   - ☐ Information on side effects (adverse events) you may experience, and how these were treated;
   - ☐ Long-term information about your general health status and the status of your disease;
   - ☐ Data that may be related to tissue and/or blood samples that may be collected from you
   - ☐ Codes that will identify you, such as your social security number and medical record number.
   - ☐ Mental health information including drug and alcohol history
   - ☐ Communicable disease information like HIV and Hepatitis history

You may request a blank copy of data forms from the study doctor or his/her research staff to learn what kind of information might be shared.

7. How will my personal health information be used?

The University of Colorado Colorado Springs researchers will use your health information for research. As part of this research, they may give your information to the following sponsor and/or "group(s)" taking part in the research. The researchers may also permit staff from this sponsor and/or "group(s)" to review your original records as required by law for audit purposes.

RELEASE/DISCLOSE TO: (Investigator please add/remove bullets per your protocol)

- The Study Sponsor
- University of Colorado Colorado Springs including the Institutional Review Board (IRB)
- The research coordinating centers, core laboratories, and imaging processing center, all of whom are involved in the conduct of the research
- The Cooperative Group
- The Office of Human Research Protection (OHRP), and other government agencies involved in keeping research safe for people

8. How will information about me be kept private?

Law requires University of Colorado Colorado Springs, its member clinics and allied health professionals, the investigators, and any other healthcare providers to protect your health information, except as allowed by law, their Notice of Privacy Practices, and this authorization. However, your information may be shared with other organizations that are not required to follow federal privacy laws. Healthcare providers, from University of Colorado Health, cannot assure you that the information will remain protected and will not be further disclosed by other organizations.

9. If I sign this form, will I automatically be in the research study?

No, there will be further discussion and a separate consent to sign if you are selected to participate in the study. After discussion, you may decide to take part in the research study. At that time, you will be asked to sign a specific research consent form. If you do not sign this form, you cannot participate in the Study.

10. Can I withdraw my permission?

You can change your mind at any time and withdraw your permission to allow your personal health information to be used in the research. If this happens, you must withdraw your permission in writing. Beginning on the date you withdraw your permission, no new personal health information will be used for the research study. However, University of Colorado Colorado Springs will not be able to retrieve any health information that has already been released. Researchers may continue to use the health information that was provided before you withdrew your permission.

If you sign this form and enter the research study, but later change your mind and withdraw your permission, you will be removed from the research study at that time.

To withdraw your permission, please contact the person below. He/she will make sure your written request to withdraw your permission is processed correctly.

Title and Name of Contact Person:
Address:
Phone: **FAX Number:**

11. What are my rights regarding access to my personal health information?

You have the right to refuse to sign this permission form. You have the right to review and/or copy records of your health information kept by University of Colorado Colorado Springs. You do not have the right to review and/or copy research study records kept by the study sponsor or other researchers associated with the research study.

12. How long will this permission last?

If you agree, by signing this form, that researchers can use your personal health information, this permission has no expiration date. However, as stated above, you can change your mind and withdraw your permission at any time.

(Signature Page on Next Page)

AUTHORIZATION SIGNATURE PAGE

Authorization Approval and Receipt Acknowledgement:

I hereby authorize the use or disclosure of the health information described in this authorization and acknowledges receiving a signed copy of this authorization. I understand that if anyone who receives my health information is not a health care provider or a health plan, my health information may not be protected by federal privacy laws if my health information is re-disclosed by that recipient person or University of Colorado Colorado Springs.

Signature:_____ **Date**: _____

Print Name: _____

Address: _____

_____

Phone: _____

Include the following only when the Study Subject is unable to consent

Authorization must be signed by the participant or by the parent/legal guardian or a minor, or by the legal representative when the participant lacks decisional capacity, or if the participant is physically unable to sign but mentally understands and consents.

Basis for legal authority to sign this authorization by a personal representative:

State relationship (Parent, Guardian, Legal Representative): _____

Witness:

Signature: _____

Print Name: _____

Date: _____

University of Colorado Colorado Springs

Request for Waiver of Elements of Authorization or an Altered Authorization

Date of Request:	Principal Investigator ("PI"):
Title of Research Project:	
Mailing Address:	
PI's email:	PI's Phone Number:

Instructions: In order for the Privacy Board to approve a waiver of HIPAA process or a partial waiver of any of the required elements of HIPAA, Federal Regulation 45CFR 164.512(i) requires the following:

Does your study involve the use or disclosure of protected health information (PHI)?
☐ Yes ☐ No
PHI = individually identifiable health information that is collected for treatment, diagnosis, or research purposes.

If yes, check off any of the following identifiable information you will be obtaining.

- ☐ Patient/Subject Name
- ☐ Medical device Identifiers
- ☐ Electronic Mail (Email Address)
- ☐ Address town or city*
- ☐ Internet protocols (IP) address
- ☐ Medical record numbers
- ☐ Address zip code*
- ☐ Full face photographic images
- ☐ Account numbers
- ☐ Fax number
- ☐ Address street location
- ☐ Web URL's
- ☐ Social security number
- ☐ Address state*
- ☐ Biometric identifiers (finger/voice prints)
- ☐ Health plan beneficiary numbers
- ☐ Telephone
- Certificate/license numbers
- ☐ Elements of dates (except yr.) related to person, i.e., date of admission or discharge dates, date of death*
- ☐ Any unique identifying number, characteristic or code
- ☐ Vehicle identification numbers and serial numbers including license plates
- ☐ Link to identifier (code)
- ☐ None of the above listed items will be recorded

Are you obtaining this information for recruitment purposes? ☐ Yes ☐ No
Are you obtaining this information for study purposes (i.e. data analysis, follow-up)? ☐ Yes ☐ No

Under Privacy rule provisions, research data that includes any of the 18 identifiers listed above cannot be considered de-identified. Authorization from the subject or a waiver of authorization granted by the UCCS Privacy Board is required. Items with an asterisk (*) may be included and considered a "limited data set." Use of data under the provision of a "limited data set" requires the signing of a data use agreement by the recipient (this includes researchers) and a request for a waiver of authorization.

University of Colorado Colorado Springs

REQUEST FOR WAIVER OF HIPAA AUTHORIZATION

According to HIPAA Privacy Rule regulations, in order to use or disclose an individual's PHI in the conduct of research without the express authorization of the individual, all of the following criteria must be met.

A. The use of disclosure of PHI involves no more than minimal risk to the privacy of individuals, based on, at least, the presence of the following elements:
- An adequate plan to protect the identifiers from improper use or disclosure.
- An adequate plan to destroy the identifiers at the earliest opportunity consistent with the conduct of the research, unless there is a health or research justification for retaining the identifiers, or such retention is otherwise required by law; **AND**
- Adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, (except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of PHI would be permitted by regulation).

B. The research could not practicably be conducted without the alteration or waiver; **AND**

C. The research could not practicably be conducted without access to and use of the PHI.

Does your study meet all the above criteria for a waiver of HIPAA authorization? ☐ Yes ☐ No

Does your study qualify for a waiver of authorization using a limited data set (i.e. you checked only those boxes indicated with an asterisk (*)? ☐ Yes ☐ No
If yes, please attach a completed Data Use Agreement.

As PI of the research project indicated on this form, I make the following assurances to the UCCS Privacy Board:

☐ The PHI for which use or disclosure is sought is necessary for research purposes.

☐ I will provide the UCCS Privacy Board with written notification if any of the responses to the above questions change.

☐ I understand that the UCCS Privacy Board is NOT an Institutional Review Board and is not authorized to review and/or approve human subject's research regulated under the Common Rule.

☐ I understand that the above representations are binding upon and will inure to the benefit and obligation of the PI of the research project indicated on this form and his/her respective successors and/or assigns.

I will apply the above conditions to PHI maintained by the UCCS Covered Entity or Covered Component.

_____ _____

Principal Investigator Signature Date

University of Colorado Colorado Springs

ACTIVITIES PREPARATORY TO RESEARCH
REQUEST FOR WAIVER OF AUTHORIZATION

Date of Request:	Principal Investigator ("PI"):
Title of Research Project:	
Mailing Address	
PI's email:	PI's Phone Number:

Instructions: In order for the Privacy Board to approve a request for activities preparatory to research and waive any of the required elements of the Health Insurance Portability and Accountability Act ("HIPAA") please provide the following information.

1. Provide a brief description of the research project.

2. Please clearly list the minimal amount of Protected Health Information ("PHI") necessary to conduct your research project.

I acknowledge that the HIPAA Privacy Rule imposes the following restrictions [45 CFR 164.512(i)(1)(ii)] on the use of PHI in activities preparatory to research, defined as:

- ☐ The development of research questions;
- ☐ The development of eligibility (inclusion and exclusion) criteria; and
- ☐ The determination of study feasibility and design (in terms of the available number and eligibility of potential study participants).

I therefore agree that:

- ☐ I will engage in preparatory to research activities only when necessary.
- ☐ I will review only the PHI that is necessary to prepare a research protocol for grant preparation or IRB review or for those preparatory to research activities listed above.
- ☐ I will not remove any PHI, abstracted in the course of my review of PHI, from the Covered Entity or Covered Component. Furthermore, I will not disclose the abstracted PHI under any circumstances to anyone outside of the Covered Entity or Covered Component.

I will apply the above conditions to PHI maintained by the UCCS Covered Entity or Covered Component.

_____ _____

Principal Investigator Signature Date

University of Colorado Colorado Springs

Required Representations for
Research on Decedent's Information

Date of Request:	Principal Investigator ("PI"):
Title of Research Project:	
Mailing Address	
PI's email:	PI's Phone Number:

Instructions: In order for the Privacy Board to approve a request for activities preparatory to research and waive any of the required elements of the Health Insurance Portability and Accountability Act ("HIPAA") please provide the following information.

1. Provide a brief description of the research project.

2. Please clearly list the minimal amount of Protected Health Information ("PHI") necessary to conduct your research project.

As PI of the research project indicated on this form, I make the following assurances to the UCCS Privacy Board:

☐ The use or disclosure sought is solely for research on the PHI of decedents.

☐ Documentation of death of each of the individuals whose information will be used for this project can and will be provided to the UCCS Privacy Board immediately upon request.

☐ The PHI for which use or disclosure is sought is necessary for research purposes.

☐ I will provide the UCCS Privacy Board with written notification if any of the responses to the above questions change.

☐ I understand that the UCCS Privacy Board is NOT an Institutional Review Board and is not authorized to review and/or approve human subject's research regulated under the Common Rule.

☐ I understand that the above representations are binding upon and will inure to the benefit and obligation of the PI of the research project indicated on this form and his/her respective successors and/or assigns.

I will apply the above conditions to PHI maintained by the UCCS Covered Entity or Covered Component.

_____ _____

Principal Investigator Signature Date

DATA USE AGREEMENT

This Agreement is entered into by and between the **Regents of the University of Colorado, a body corporate, for and on behalf of the University of Colorado Colorado Springs (“UCCS”) HealthCircle Clinics ("UCCS HealthCircle Clinics")** and the Recipient **("Recipient")** named on Schedule 1 (attached hereto and by this reference incorporated herein) as of the Effective Date noted on **Schedule 1**.

A. UCCS HealthCircle Clinics are providing certain Protected Health Information ("PHI") to Recipient in the form of a Limited Data Set for the purpose(s) identified in paragraphs 4 and 5 of **Schedule 1**.

B. In connection with the provision of that PHI, pursuant to the Health Insurance Portability and Accountability Act and regulations promulgated pursuant thereto (collectively "HIPAA"), UCCS HealthCircle Clinics are required to obtain assurances from Recipient that Recipient will only use or disclose PHI as permitted herein.

C. The parties enter into this Agreement as a condition to UCCS HealthCircle Clinics’ furnishing the Limited Data Set to Recipient, and as a means of Recipient's providing assurances about use and disclosure. The provisions of this Agreement are intended to meet the Date Use Agreement requirements of HIPAA.

NOW THEREFORE, the parties agree as follows:

1. Definitions. Each capitalized term used in this Agreement and not otherwise defined, shall have the meaning given it in HIPAA.

2. Term. This Agreement shall commence on the Effective Date and continue until terminated in accordance with Section 4 below.

3. Recipient's Obligations. Recipient shall:

a. Comply with all applicable federal and state laws and regulations relating to the maintenance of the PHI, the safeguarding of the confidentiality of the PHI, and the use and disclosure of the PHI;

b. Use and disclose the PHI only for the purpose(s) identified in paragraph 4 and 5 of **Schedule 1**, as otherwise required by law, and for no other purpose;

c. Use appropriate safeguards to prevent the use and disclosure of the PHI, other than for a use or disclosure expressly permitted by this Agreement;

d. Immediately report to the UCCS HealthCircle Clinics any use or disclosure of the PHI other than as expressly allowed by this Agreement;

e. Ensure that its employees and representatives comply with the terms and conditions of this Agreement, and ensure that its agents, Business Associates and subcontractors to whom Recipient provides the PHI agree to comply with the same restrictions and conditions that apply to Recipient hereunder;

f. Not identify or attempt to identify the information contained in the Limited Data Set, nor contact any of the individuals whose information is contained in the Limited Data Set;

g. Not request use, or disclose more PHI than the minimum amount necessary to allow Recipient to perform its functions pursuant to the purpose identified in **Schedule 1;** and

h. Indemnify, defend and hold UCCS and the UCCS HealthCircle Clinics harmless from all costs and expenses (including attorney fees) that relate to a breach of Recipient's obligations.

4. Termination. UCCS HealthCircle Clinics may terminate this Agreement and any disclosures of PHI pursuant hereto, upon 10 days' notice to Recipient, if Recipient violates or breaches any material term or condition of this Agreement. UCCS HealthCircle Clinics may terminate this Agreement without cause upon 30 days' written notice. Upon termination, Recipient shall promptly return or destroy the Limited Data Set received from HealthCircle Clinics in connection with the purpose identified on **Schedule 1**. If return or destruction of the Limited Data Set is not feasible, Recipient shall continue the protections required under this Agreement for the Limited Data Set consistent with the requirements of this Agreement and applicable HIPAA privacy standards. If Recipient ceases to do business or otherwise terminates its relationship with HealthCircle Clinics, Recipient agrees to promptly return or destroy all information contained in the Limited Data Set received from HealthCircle Clinics in a timely manner.

5. Governing Law and Venue. This Agreement shall be governed by the laws of the State of Colorado. Venue for any claim, action or suit, whether state of federal, between Recipient and HealthCircle Clinics shall be El Paso County, Colorado.

[Remainder of this page left blank intentionally]

IN WITNESS WHEREOF, the parties have executed this Agreement effective as of the Effective Date.

UCCS HealthCircle Clinics:	**Recipient:**
By:_____	By: _____
Title:_____	Title: _____
Date:_____	Date: _____

Schedule 1

1. Effective Date: _____

2. Name of HealthCircle Clinic/Person Releasing the Limited Data Set:
_____

3. Name of Recipient of the Limited Data Set:
_____

4. Purpose of Limited Data Set Disclosure:

- ❑ Research Study

  Title:_____

  Principal Investigator: _____

  IRB #: _____

  Sponsor: _____

- ❑ Public Health

- ❑ Health Care Operations (i.e., Quality improvement, teaching, accreditation, the development of clinical guidelines.)

5. The recipient of the LDS listed in #2 is permitted to use and disclose the LDS for the following purpose(s):

UCCS HealthCircle
UNIVERSITY OF COLORADO
COLORADO SPRINGS

Notice of Privacy Practices
Effective: July 1, 2015

Your Information. Your Rights. Our Responsibilities.

This notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please read it carefully.

The University of Colorado Colorado Springs HealthCircle Clinics to include:

- Center for Active Living
- The Aging Center
- Primary Care Clinic
- Peak Nutrition Clinic
- Veterans Health and Trauma Clinic

The following are included as a part of these clinics:

- Any health care professional who treats you at any of our locations;
- All departments and units of the University of Colorado Colorado Springs that must use your medical information as a part of their job;
- All employees, volunteers, and staff of the University of Colorado Colorado Springs;
- Any business associate who performs work for the HealthCircle Clinics that requires them to access to your medical information;
- All students in certified training programs.

All of these entities, sites, and locations will follow what is described in this notice. In addition, they may share medical information with each other for your treatment, payment, or their health care operations described in this notice.

Your Rights

You have the right to:

- Get a copy of your paper or electronic medical record
- Amend your paper or electronic medical record
- Request confidential communication
- Ask us to limit the information we share
- Get a list of those with whom we've shared your information
- Get a copy of this privacy notice
- Choose someone to act for you
- File a complaint if you believe your privacy rights have been violated

Your Choices

You have some choices in the way that we use and share information as we:

- Tell family and friends about your condition
- Provide disaster relief
- Include you in a directory
- Provide mental health care
- Market our services
- Raise funds

Our Uses and Disclosures

We may use and share your information as we:

- Treat you
- Run our organization
- Bill for your services
- Help with public health and safety issues
- Do research
- Comply with the law
- Respond to organ and tissue donation requests
- Work with a medical examiner or funeral director
- Address workers' compensation, law enforcement, and other government requests
- Respond to lawsuits and legal actions

Your Rights

When it comes to your health information, you have certain rights. This section explains your rights and some of our responsibilities to help you.

Get an electronic or paper copy of your medical record

- You can ask to see or get an electronic or paper copy of your medical record and other health information we have about you. Ask us how to do this.
- We will provide a copy or a summary of your health information, usually within 30 days of your request. We may charge a reasonable, cost-based fee.

Ask us to amend your medical record

- You can request to amend health information about you that you think is incorrect or incomplete. Ask us how to do this.
- We may say "no" to your request, but we'll tell you why in writing within 60 days.

Request confidential communications

- You can ask to be contacted in a specific way (for example, home or office phone) or to send mail to a different address.
- We will say "yes" to all reasonable requests.

Ask us to limit what we use or share

- You can request that we not use or share certain health information for treatment, payment, or our operations. We are not required to agree to your request, and we may say "no" if it would affect your care.
- If you pay for a service or health care item out-of-pocket in full at time of service, you can ask us not to share that information for the purpose of payment or our operations with your health insurer. We will say "yes" unless a law requires us to share that information.

Get a list of those with whom we've shared information

- You may request a list (accounting) of the times we've shared your health information for six years prior to the date you ask, who we shared it with, and why.
- We will include all the disclosures except for those about treatment, payment, health care operations, and certain other disclosures (such as any you asked us to make). We'll provide one accounting a year for free but will charge a reasonable, cost-based fee if you ask for additional copies within 12 months.

Get a copy of this privacy notice

You may request a paper copy of this notice at any time, even if you have agreed to receive the notice electronically. We will provide you with a paper copy promptly.

Choose someone to act for you

- If you have given someone medical power of attorney or if someone is your legal guardian, that person can exercise your rights and make choices about your health information.
- We will make sure the person has this authority and can act on your behalf before we take any action.

File a complaint if you feel your rights are violated

- If you feel your rights have been violated in any way, you may contact our Privacy Officer via phone (719) 255-3837 or email doconnor@uccs.edu
- The University of Colorado Colorado Springs also maintains a confidential reporting hotline, which may be accessed at: www.ethicspoint.com
- You can file a complaint with the U.S. Department of Health and Human Services Office for Civil Rights by sending a letter to 200 Independence Avenue, S.W., Washington, D.C. 20201, calling 1-877-696-6775, or visiting **www.hhs.gov/ocr/privacy/hipaa/complaints/.**
- You can file a complaint with the U.S. Department of Health and Human Services Office for Civil Rights in Colorado by sending a letter to 999 18TH Street, South Terrace, Suite 417, Denver, Colorado 80202 or by calling 303-844-7915.
- Complaints to the U.S. Department of Health and Human Services must be filed within 180 days of when you learn of or should have known about the violation.
- We will not retaliate against you for filing a complaint.

Your Choices

For certain health information, you can tell us your choices about what we share. If you have a clear preference for how we share your information in the situations described below, please let us know. In these cases, you have both the right and choice to tell us to:

- Share information with your family, close friends, or others involved in your care
- Share information in a disaster relief situation
- Include your information in a hospital directory

If you are not able to tell us your preference (for example, if you are unconscious), we may share your information if we believe it is in your best interest. We may also share your information when needed to lessen a serious and imminent threat to health or safety.

In these cases, we never share your information unless you give us written permission:

- Marketing purposes
- Sale of your information
- Most sharing of psychotherapy notes

In the case of fundraising:
We may contact you for fundraising efforts related to UCCS. Information used may include your name, address, phone number, the dates you received services, department(s) from which you received services, your treating provider(s), outcome information, and health insurance status. You may request not to be contacted again and your choice to opt-out will not be a condition of treatment or payment.

Our Uses and Disclosures

How do we typically use or share your health information?
We typically use or share your health information in the following ways:

To treat you
We can use your health information and share it with other professionals who are treating you.
Example: A doctor treating you for an injury asks another doctor about your overall health condition.

To run our organization
We can use and share your health information to run our practice, improve your care, and contact you when necessary.
Example: We use health information about you to manage your treatment and services.

To bill for your services
We can use and share your health information to bill and get payment from health plans or other entities.
Example: We give information about you to your health insurance plan so it will pay for your services.

How else can we use or share your health information?

We are allowed or required to share your information in other ways – usually in ways that contribute to the public good, such as public health and research. We have to meet many conditions in the law before we can share your information for these purposes.
For more information, see: www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/index.html.

Help with public health and safety issues
We can share health information about you for certain situations such as:

- Preventing disease
- Helping with product recalls
- Reporting adverse reactions to medications
- Reporting suspected abuse, neglect, or domestic violence
- Preventing or reducing a serious threat to anyone's health or safety

Do research
We can use or share your information for health research.

Comply with the law
We will share information about you subject to state or federal law. Your information may also be shared with the Department of Health and Human Services to ensure our compliance with federal privacy law.

Respond to organ and tissue donation requests
We can share health information about you with organ procurement organizations.

Work with a medical examiner or funeral director
We can share health information with a coroner, medical examiner, or funeral director when an individual dies.

Address workers' compensation, law enforcement, and other government requests
We can use or share health information about you:

- For workers' compensation claims
- For law enforcement purposes or with a law enforcement official
- With health oversight agencies for activities authorized by law
- For special government functions such as military, national security, and presidential protective services

Respond to lawsuits and legal actions
We can share health information about you in response to a court or administrative order, or in response to a subpoena.

UCCS HealthCircle
UNIVERSITY OF COLORADO
COLORADO SPRINGS

Our Responsibilities

- We are required by law to maintain the privacy and security of your protected health information.
- We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information.
- We must follow the duties and privacy practices described in this notice and provide you with a copy.
- We will not use or share your information other than as described above, unless you indicate otherwise in writing. Any subsequent changes to the sharing of your information must also be submitted in writing.

For more information see:
www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/noticepp.html

Changes to the Terms of this Notice

We can change the terms of this notice, and the changes will apply to all information we have about you. The new notice will be available upon request, in our office, and on our web site.

Contact Information

Deborah O'Connor, HIPAA Privacy Officer
University of Colorado Colorado Springs Privacy Officer:
1420 Austin Bluffs Parkway
Colorado Springs, CO 80918
Telephone 719-255-3837
Email doconnor@uccs.edu

University of Colorado Colorado Springs

Privacy Complaint Form

I,_____(Patient Name), hereby register this privacy-related complaint to_____(Name of Health Care Provider). Under federal law 104-191, also known as HIPAA, I am entitled to register such a complaint in writing to my health care provider.

Policies and Limitations on Privacy–related Complaints

We value your trust and confidence in us as your healthcare provider. Therefore, we ask that you file a Complaint directly with us first and give us the opportunity to resolve the issue or problem promptly. We will investigate and act on your Complaint promptly.

- Federal law also gives you the right to file a privacy complaint with the Secretary of the US Department of Health and Human Services (DHHS) in Washington, DC. You may file such a complaint in writing via email or the Internet.
- Under federal law and our own policies, there will be no retaliation against you for filing a compliant
- To be valid, complaints must be filed within 180 days of when the privacy-related violation occurred. Only the Secretary of the US Department of Health and Human Services can waive this time requirement.

Please describe your complaint below, or attach a separate page(s) to describe your complaint:

Patient Name: _____

Address: _____

_____

_____

Telephone: _____

Email: _____

_____
Signature of Patient or Personal Representative

_____
Name of Patient or Personal Representative

_____
Date

_____
Description of Personal Representative's Authority (if applicable)

▼▼▼ FOR OFFICE USE ONLY ▼▼▼

Received by:		
Date Received:	**Time Received**:	
Action(s) Taken:		
Investigation Results:		
Patient Follow-Up:		
Approved By:		

University of Colorado Colorado Springs

PRIVACY-SECURITY INCIDENT REPORT

SECTION I – GENERAL INFORMATION

Name of Staff Member Reporting Incident			
Telephone Number		**Email Address**	
Division/Office/Facility			
Unit/Section			
Supervisor			

SECTION II – PRIVACY INCIDENT INFORMATION

Date of Incident _____ **Time of Incident** _____ **Location of Incident** _____

Description of Incident (Include the names of those involved in the privacy incident.)

Incident also reported to

Signature/Title: _____ **Date:** _____

(Staff member reporting privacy incident)

Supervisor Comments

Signature/Title: _____ **Date:** _____

(Supervisor of staff member reporting privacy incident)

Routing Information: Agency Staff→Staff Supervisor→ Agency Privacy Official/Designee→DHHS Privacy Officer

SECTION III - INCIDENT DISPOSITION

Tracking Information

Clinic Name	**Incident Number**
Tracking Number from Privacy Complaint Form, if applicable	

Privacy Incident Classification

☐ **Unauthorized Access** (Paper)	☐ **Unauthorized Access** (Electronic)
☐ **Unauthorized Disclosure Outside Entity**	☐ **Inappropriate Use Within Entity**
☐ **Unauthorized Use or Disclosure by Business Associate**	☐ **Improper Communications** (Mail, E-mail, Fax, Phone)
☐ **Improper Denial/Fulfillment of Client Rights**	☐ **Improper Oral Communications**
☐ **Improper Disposal**	☐ **Improper Password Management**
☐ **Other** (Specify)	

Severity of Privacy Incident (check one)

☐ **Severe** (Press may be involved. Affects patients, clients and/or public, business associate(s). **Must be immediately routed to UCCS Privacy Officer for resolution.**

☐ **Moderate** (Press involvement unlikely. Affects UCCS, and/or business associate(s). Forward to UCCS Privacy Officer for disposition if privacy incident cannot be resolved within the agency.)

☐ **Low** (No affect outside of Entity. Forward to UCCS Privacy Officer for tracking. Entity able to resolve internally.)

Privacy Incident Analysis (Investigation notes, including potential harm to client and potential risk to Entity/others.)

Four factors must be considered, at minimum:

1. The nature and extent of the PHI involved -- Was sensitive data, such as Social Security numbers and detailed clinical information, involved in an incident?
2. The unauthorized person who used the PHI or to whom the disclosure was made -- If the disclosures were to another HIPAA-regulated entity or to a federal agency, for example, this may result in a "lower probability that the [PHI] has been compromised since the recipient of the information is obligated to protect the privacy and security of the information in a similar manner as the disclosing entity."
3. Whether the PHI actually was acquired or viewed -- This would typically involve a forensic analysis or investigation that could determine whether PHI contained on a lost or stolen laptop or other portable electronic device actually was viewed or accessed.
4. The extent to which the risk to the PHI has been mitigated -- This might involve reaching out to an unauthorized recipient of the PHI to obtain "satisfactory assurances" that any PHI sent to a recipient was not further used or disclosed but instead destroyed.

Incident Analysis...

Action To Be Taken (All Incident Reports must be forwarded to UCCS Privacy Officer for review)

To be resolved by UCCS Privacy Officer

Additional staff training needed (Specify)

Policies or Procedures to be reviewed/updated (Specify)

Employee Sanctions (Specify)

Notify Patient(s), OCR, FTC, or Media (Specify)

Record disclosure in accounting of disclosures log.

Other (Specify)

Signature/Title:_____ **Date:** _____

(Privacy Officer/Designee)

SECTION IV – UCCS PRIVACY OFFICER REVIEW

Privacy Incident Analysis (Enter notes related to investigation or review.)

Action(s) to Be Taken

Incident determination is accurate and resolution complete – Report filed

Additional action(s) needed (Specify)

UCCS Policies and/or Procedures to be reviewed/updated (Specify)

New UCCS Policy needed (Specify)

Other (Specify)

Report Forwarded To

	Office of Legal Counsel	
	UCCS Management (Specify)	
	Other Personnel (Specify)	
	Other (Specify)	

Signature/Title:_____ **Date:** _____

(UCCS Privacy Officer)

SECTION V – COMMUNICATIONS LOG

Communications				
Incident Number			**Incident Classification**	
Date	**Delivered By/ Organization**	**Mode**	**Received By/ Organization**	**Summary of Communication**

Communications

Incident Number **Incident Classification**

Date	Delivered By/ Organization	Mode	Received By/ Organization	Summary of Communication

University of Colorado Colorado Springs

Patient Name(s):
Medical Record #:
Date of Birth:
Contact Phone #:

REVOCATION OF AUTHORIZATION

Revocation from (please check all that apply):

☐ Aging Center (719) 255-8002 (719) 255- 8006 Fax	☐ Center for Active Living (719)255-8004
☐ Peak Nutrition Clinic (719) 255- 7524	☐ Primary Care Clinic (719) 255- 8001 (719) 255- 8044 Fax
☐ Veterans Health and Trauma Clinic (719) 255- 8003 (719) 255- 8075 Fax	☐ Helen and Arthur E. Johnson Beth-El College of Nursing and Health Sciences, Nurse Family Partnership© (719) 255-8049

I,_____(Patient Name), want to revoke the authorization that I gave to

_____(List name of person or unit or department of the UCCS HealthCircle Clinics to which you gave authorization, if known) on or about_____(Date) which gave UCCS HealthCircle Clinics the authority to give my information to _____ (Name of recipient of information, if known).

_____
Signature of Patient or Authorized Representative

_____
Printed Name

_____
Date of Signature

_____
Relationship to Patient (if applicable)

University of Colorado Colorado Springs

Patient Name(s)
Medical Record #
Date of Birth
Contact Phone #

Request for Accounting of Disclosures of Protected Health Information

I,_____(Print Name), request an accounting for disclosures of my health or billing information:

For the period: FROM:_____TO: _____

Name of Provider(s) seen: _____

Send accounting to:

- ☐ Address: _____
- ☐ I will pick up the accounting in person. Please contact me at_____(telephone number) when document(s) is/are ready.
- ☐ Fax Number: _____

I understand that this accounting for disclosures will include all disclosures ***except*** those:

- To those for whom use and disclosure of my health information was made to carry out my treatment, process payment for my health care, or carry out UCCS's Covered Entities health care business operations.
- To myself or my personal representative.
- Incidental disclosures made in connection with a use or disclosure otherwise permitted or required by HIPAA.
- To persons involved in my care or as part of an inpatient directory.
- Pursuant to an authorization for release of information signed by myself or my personal representative.
- For national security or intelligence purposes, to correctional institutions, or to law enforcement officials under certain circumstances.
- To correctional institutions or law enforcement officials under certain circumstances.
- As part of a limited data set, when the recipient has executed a data use agreement, disclosed for research, public health, or certain health care operations purposes.
- That occurred prior to April 14, 2003 or that designated site becoming a HIPAA covered entity.

I understand that this accounting will include all disclosures of HIV-related information except disclosures made to:

- federal, state, or local health officers that are required or permitted by law.
- persons reviewing information or records in the ordinary course of ensuring that a health facility is in compliance with applicable quality of care standards, program evaluation, program monitoring or service review.
- life and health insurers, government payers and health care centers in connection with underwriting and claim activity for life, health, and disability benefits.

I understand that I may receive the first accounting for disclosures within a 12-month period at no charge. I understand that if I am requesting a second or subsequent accounting in a 12-month period, I will be charged a flat fee for this accounting. This fee is to cover the cost of supplies, labor and postage associated with copying. I further understand that if I do not ask you to proceed with my request, I may modify my request to reduce the fee or withdraw my request and pay no fee.

_____

Signature of Patient or Authorized Representative

_____

Name of Patient or Authorized Representative

_____

Date

_____

Relationship to Patient (if applicable)

University of Colorado Colorado Springs

Request for Amendment of Health Information

Instructions

To submit a request for amendment, please complete, sign and return the attached form to:

Director – (Insert Clinic Name)
UCCS HealthCircle Clinics
Lane Center for Academic Health Sciences
4863 North Nevada Ave.
Colorado Springs, CO 80918

The attached form may be used to request an amendment to a record of your medical care. We are required to amend your medical record, upon written request, unless:

(1) we did not create the information;
(2) we do not maintain the information as part of your record;
(3) we determine that the information is accurate and complete as currently recorded; or
(4) the information is the type that would not be available to you for inspection.

Please be aware that under no circumstances will we delete or alter the original documentation in the medical record. Any amendments made to the medical record will be appended in the appropriate part of the record.

If we did not create the information that you want to amend, you may submit reasonable evidence that the person or organization that originally created the information at issue is not available, and the UCCS designated healthcare competent will consider your request.

The UCCS covered entity responds to requests for amendment within sixty (60) days of receiving the written request. You may expect to receive a response or a notification of delay within that approximate time frame. If we deny your request to amend, you may submit a written statement of rebuttal, which will be included in all subsequent disclosure of the information at issue. If you choose not to submit a statement of rebuttal, a copy of this request for amendment will be included in all subsequent disclosures of that information.

For more information about amending a medical record, you may contact the UCCS HIPAA Privacy Officer at 719-255-3837, who will assist you in contacting the correct individual.

Note that requests for amendment must be made in writing and will not be accepted over the telephone.

Request for Amendment of Health Information

Today's date_____

Patient's Name_____

Medical record number if known_____

Birth Date _____

Address_____

Phone (home)_____Phone (work) _____

Describe the information that you would like to have amended (physician notes, etc.).

On what date(s) was the care that is described in the record provided?

What is incorrect about the record? What would you like to change or add to the record?

To your knowledge, has anyone received or relied on this information (e.g. your doctor, another health care provider, and insurance company, attorney)? If yes, please provide the name(s) and address(es) of those individuals or organization so that Clinic may inform them of any amendments.

Signature:_____Date_____

If you are not the patient, please fill in the following:

Your Name_____

Relationship to Patient_____

Address_____

Phone (home)_____Phone (work)_____

Signature_____Date _____

University of Colorado Colorado Springs

Approval of Request To Amend Medical or Billing Records

After carefully considering your request to amend your Protected Health Information dated _____, UCCS HealthCircle Clinics has determined that the amendment is appropriate.

The following steps will be taken to amend the record:

1. The information in your record(s) that is affected by the change will be identified. HealthCircle Clinic will insert an amendment to that information or link that information to a description of the information as amended.
2. We will notify any individual that you identify as having received the Protected Health Information who needs the amended information and any individual within HealthCircle Clinics knows has the Protected Health Information that is being amended and who has relied on that information.

University of Colorado Colorado Springs

Denial of Request to Amend Healthcare Information

After carefully considering your request to amend your Protected Health Information dated _____, _____(Name of Clinic) has determined that amendment of the information is not appropriate at this time because:

☐ The Clinic did not create the information that you wish to amend, and you have not supplied us with reasonable information indicating that the person who did create the information is no longer available to amend the information.

☐ We do not maintain the information that you want amended in our records.

☐ The information that you have asked to amend is information that is not available for inspection by patients or their representatives.

☐ The Clinic has determined that the information you want to amend is accurate and complete.

You may submit a written statement of rebuttal to the Director of the Clinic or Designate who will be included in all subsequent disclosures of the information at issue. If you choose not to submit a statement, we will include a copy of your request for amendment in all subsequent disclosures of that information.

If you are dissatisfied with the determination to deny your request for amendment, you may submit a complaint to:

Director of Campus Compliance/Privacy Officer
University of Colorado Colorado Springs
Main Hall Suite 416C
1420 Austin Bluffs Pkwy
Colorado Springs, CO 80918

or to:

Velveta Howell, Regional Manager
Office for Civil Rights
U.S. Department of Health and Human Services
1961 Stout Street -- Room 1426 FOB
Denver, CO 80294-3538
Voice Phone (303)844-2024
FAX (303)844-2025
TDD (303)844-3439

University of Colorado Colorado Springs

Request to Restrict Uses or Disclosures of Personal Medical Records

I,_____(Patient Name), hereby request to restrict certain uses or disclosures of my medical records from_____(Name of Practice or Physician). Under federal law 104-191, also known as HIPAA, I am entitled to such restrictions of uses or disclosures upon written request.

I request the following restriction(s) on uses and disclosures of my personal medical records:

Policies and Limitations on Restrictions of Uses and/or Disclosures

- Under federal law, while you have the right to request restrictions on uses or disclosures of your personal medical records, we must accept and comply with your written request if:
  - Except as otherwise required by law, the disclosure is to a health plan for the purpose of carrying out payment of health care operations (and is not for purposes of carrying out treatment); and,
  - The personal medical information pertains solely to a health care item or service for which we have been paid out-of-pocket in full.
- Upon accepting your request, we must abide by it, except in emergency situations where a use or disclosure is necessary to provide treatment.
- Under federal law, restrictions on use or disclosure do not apply to the following types of uses and disclosures, for which no consent, authorization, nor opportunity to agree or object is required:
  - Public Health
  - Abuse
  - Neglect or Domestic Violence Reporting
  - Health Oversight
  - Judicial or Administrative Proceedings
  - Law Enforcement
  - Research under Privacy Board or IRB Waiver
  - Immediate Threats to Public Safety
  - Government Functions; or
  - Uses and Disclosures otherwise required by Law.
- We may terminate our agreement to restrictions if:
  - You agree to or request the termination in writing

- You request the termination verbally (we will document your verbal request to terminate restrictions)
- We inform you that we are terminating our agreement to restrictions (such termination is only effective for information created or received *after* we inform you of our termination)

Patient Name: _____

Address: _____

_____

_____

Telephone: _____

Email: _____

_____ _____

Signature of Patient or Personal Representative Date

_____

Printed Name of Patient or Personal Representative

_____

Description of Personal Representative's Authority

▼▼▼ FOR OFFICE USE ONLY ▼▼▼

Received by:			
Date Received:		**Time Received:**	
Action(s) Taken:			
Records Flagged for Restriction(s):			
Patient Follow-Up:			
Staff Signature:			

University of Colorado Colorado Springs

Request for Alternate Means of Communication of Confidential Medical Information

---

I,_____(Patient Name), hereby request that confidential communications about my medical information or my medical records from_____(Name of Practice or Physician) be communicated to me using an alternate means or be delivered to me using an alternate location. Under federal law 104-191, also known as HIPAA, I am entitled to request such an arrangement upon written request.

I request that confidential communications be:

☐ Sent to an alternate address

Alternate Address: _____

_____

_____

_____

☐ Sent via an alternate medium, such as Fax or Registered Mail:

Describe: _____

_____

_____

Policies and Limitations on Alternate Means of Communication

- Under federal law, we are required to accommodate "reasonable" requests for communicating confidential medical to you via alternate means. We may deny your request if we determine that your request is unreasonable.
- If an expense is involved in fulfilling your request, we may charge the expense back to you, plus a small service fee. If the expense involved is unreasonable or burdensome, we may deny your request on that basis alone.
- With your request, you agree that the security and confidentiality of your confidential medical information that we send to an alternate address or via an alternate means is your responsibility alone. If we act on your request and send communications as you have specifically directed us to do in writing, you agree that we cannot and shall not be

responsible for any inadvertent disclosures that may occur as a result of fulfilling your written request.

Patient Name: _____

Address: _____

_____

_____

Telephone: _____

Email: _____

_____
Signature of Patient or Personal Representative

_____
Name of Patient or Personal Representative

_____
Date

_____
Description of Personal Representative's Authority

▼▼▼ FOR OFFICE USE ONLY ▼▼▼

Received by:			
Date Received:		**Time Received:**	
Action(s) Taken:			
Record(s) Flagged for Restriction(s):			
Patient Follow-Up:			
Approved By:			

University of Colorado Colorado Springs

Request to View or Obtain Copy of Personal Medical Records

I,_____(Patient Name), hereby request to inspect or obtain a copy of my medical records from_____(Name of Practice or Physician). Under federal law 104-191, also known as HIPAA, I am entitled to such access upon written request.

I would like to:

☐ access and inspect my personal medical records

☐ obtain a copy of my personal medical records (hardcopy records)

☐ obtain a copy of my personal medical records (electronic records)

Policies and Restrictions on Viewing or Copying Personal Medical Records

- Under federal law, we may only provide a "Designated Record Set" of your personal medical records. This Designated Record Set only includes medical and billing records we physically store and maintain on our premises, and only includes those portions of medical records that "are used to make decisions about patients."
- We are NOT able to provide you with:
    - Items not maintained in legal health records
    - Education records exempt from HIPAA
    - Psychotherapy Notes
    - Data exempted by the Clinical Lab Improvements Act
    - Data involved in criminal, civil, or administrative actions
    - Records put together in anticipation of legislation
    - Other data types may also be excluded.
- If an Electronic Health Record (EHR) system is in use, you may request and obtain an electronic copy of your medical records. You may also instruct us to send an electronic copy of your medical records to any third party you specify in writing.
- We may legally deny your request for access to your medical records, without opportunity for appeal, in the following circumstances:
    - You are an inmate in a correctional institution, and access would endanger your health and safety or the health and safety of anyone else in the facility.
    - Your records were generated in the course of ongoing research, and disclosure would jeopardize the research. (You must have agreed, in writing, to such a restriction previously. And if so, your right of access will be restored at the conclusion of the research)
    - Your records are subject to federal Privacy Act protections (Under 5 USC 552a)

    - The information was obtained from someone under a promise of confidentiality, and the access requested would be reasonably likely to reveal the source.
- We may legally deny your request for access to your medical records, but *with* an opportunity for appeal, if such access is reasonably likely to endanger the life or physical safety, or cause substantial harm to, you or another person.
- Our Policy is to respond to and fulfill your request within *30 days*.
- If you are simply viewing your Designated Record Set, we reserve certain days and times for such viewing. Our regular days and times are: Monday – Friday 8am-5pm.
- If you are requesting copies of your Designated Record Set, fees will be charged for the copies. Please check with the clinic prior to signing this document.

Patient Name: _____

Address: _____

_____

_____

Telephone: _____

Email: _____

_____
Signature of Patient or Personal Representative

_____
Printed Name of Patient or Personal Representative

_____
Date

_____
Description of Personal Representative's Authority

▼▼▼ FOR OFFICE USE ONLY ▼▼▼

Received by:			
Date Received:		**Time Received:**	
Action(s) Taken:			
Files or Records Disclosed:			
Patient Follow-Up:			
Staff Signature:			

University of Colorado Colorado Springs

Page _____

PHI Disclosure Accounting Log

Disclosure Date	Requestor Name	Patient Name	Disclosed To	Description of PHI Disclosed	Disclosure Purpose	Fee Assessed

University of Colorado Colorado Springs

HIPAA Privacy & Security Compliance Checklist

Date:	Reviewer:	Location:

Compliance Element		Yes	No	N/A	Comments
General					
1	The Notice of Privacy Practices is posted.				
2	The Notice of Privacy Practices is available upon request.				
3	The Notice of Privacy Practices is provided at the time of initial contact with UCCS.				
4	The Acknowledgement for initial receipt of Notice of Privacy Practices is obtained and documented.				
5	Telephone voicemail message volume is kept low/not audible to others.				
6	Phone conversations, speakerphone use, and dictation occur in areas where patient information is not overheard.				
7	Computer monitors are positioned in a manner that avoids access by public or others without a need to know.				
8	Computers are locked or secured when unattended.				
9	Passwords are kept secure and not posted, in desk drawer, easily accessible by others, or visible to public.				
10	Mailroom: No exposed PHI in open access mailboxes.				
11	Locked containers for shredding are used for disposing of all paper documents.				
12	Shredding containers are not over-stuffed.				
13	Trash is free of documents containing patient information.				
14	Vials containing patient names are disposed of in opaque bags.				
15	Doors to non-public areas are kept closed.				
16	Patient records are stored in a secure location.				
17	Paper medical information is not visible to public or those without a need to know.				
18	Bulletin boards and walls are free of patient medical information.				
19	Bulletin boards and walls contain only basic				

Compliance Element		Yes	No	N/A	Comments
	information, when needed, if they can be viewed by those without a need to know.				
20	Fax machines and printers used by staff are not in public areas or visible to those without a need to know.				
21	Patient information is promptly removed from faxes and printers.				
22	Fax cover sheets with confidentiality notice are used.				
23	Patient photos are only posted with authorization.				
24	After-hours access by housekeeping/other staff is restricted and/or supervised.				
Patient Care Areas					
25	Staff discussions of patients are held in areas where conversation is not easily overheard.				
26	Conversations with patient/family and friends are held in areas where information is not easily overheard.				
27	Steps are taken to ensure patient privacy when discussing care (doors closed, curtains pulled, low voices used, etc.).				
28	Documents, charts, films, and other media containing patient health information are concealed from public access and view.				
29	"Minimum necessary" information is requested on sign-in sheets, e.g. no Social Security numbers, symptoms, reason for visit.				
30	Patient information is not visible to public at sign-in desk or in waiting area.				
31	Work station is free of patient/family/visitor and inappropriate staff congregation.				
32	Whiteboards contain minimum necessary patient information.				
33	Whiteboards do not contain identifying information for silent/private patients.				
34	Whiteboards are located where they cannot be seen by those without a "need to know."				
35	Charts not in use (e.g. discharged patients) are promptly returned to Health/Medical Information Services.				
Staff Conduct					
36	Staff have read all the policies and procedures (HIPAA, etc.).				
37	Staff are aware of how to determine if a patient is "private" or not listed in the facility directory.				
38	Staff is aware of how to handle inquiries on				

Compliance Element		Yes	No	N/A	Comments
	confidential/private patients.				
39	Staff is aware of compliance/privacy hotlines and who to contact regarding a privacy concern.				
40	Staff use their own ID's and passwords.				
41	Staff wears ID badges.				
42	Desks are clear of any patient information when unattended.				
43	Staff understand that UCCS email is not encrypted and therefore should not be used to deliver any PHI				
44	Staff follow department rules related to texting patients/clients				
IT/Data Storage					
45	Portable media devices are encrypted and locked in a safe area.				
46	How is your medical record information backed up?				
47	Where is backup information stored?				
48	Do you have any outside entities doing work for your clinic that handles PHI?				
49	If yes, do we have a current signed Business Associate Agreement with them?				
Other Comments					

Introduction

This workbook contains all HIPAA Security Rule Standards and Implementation Specifications and when completed will provide procedure documentation for compliance. The UCCS Information Security Office is responsible for reviewing completed workbooks and identifying potential gaps. This document of compliance will be continually updated as we continue to improve our HIPAA compliance posture at UCCS.

Instructions for Completing this Procedures Workbook

Each covered entity at UCCS shall complete the HIPAA entity information immediately below and all "Implemented Procedures:" boxes in this workbook. Each section labeled as "(Required)" corresponds to a section of the compliance standard that must be implemented as stated for compliance. For sections labeled "(Addressable)", it must be determined whether each specification is reasonable and appropriate. If it is, it must be implemented as stated. If it is not, the entity must document the reasons for this determination and implement alternative compensating controls, or otherwise indicate how the intent of the standard can still be met. If a Standard or Implementation Specification does not apply, indicate "N/A" along with an explanation in that item's "Implemented Procedures:" box.

While each entity is ultimately responsible for their compliance with the HIPAA Security Rule, in situations where UCCS OIT or another service provider is responsible for fulfilling one or more requirements. the HIPAA entity can request verification of implementation from the service provider where this documentation is not otherwise readily available. The HIPAA requirements for which a service provider is responsible must be clearly indicated in this workbook and in any attached documentation.

HIPAA Entity Information

HIPAA Entity Name:		
Individual responsible for HIPAA Security Rule compliance:	**Name & Title:**	
Nature of electronic protected health information (ePHI) necessitating HIPAA Security Rule compliance:		
List of systems, portable devices and electronic media that contain, access or transmit ePHI:		
Last update:	**Date:**	
Reviewer Signatures:		

Table of Contents

This document is arranged by HIPAA Security Rule requirements. Each implementation specification (or Standard in the absence of specific implementation specifications) is followed by practices for compliance, along with space to document implementation of the procedures and list other supporting documentation.

HIPAA Security Rule: ADMINISTRATIVE STANDARDS

I. STANDARD

A. §164.308(a)(1)(i) - Security Management Process

It is the responsibility of each UCCS Designated Health Care Component's Leadership as well as the UCCS HIPAA Security Officer to implement policies and procedures to prevent, detect, contain, and correct security violations.

B. §164.308(a)(1)(ii)(A) - Risk Analysis (Required)

It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the Designated Health Care Component.

Practices for Compliance

1. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to identify relevant information systems and electronic information resources that require protection.
2. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to conduct risk assessments to understand and document risks from security failures that may cause loss of confidentiality, integrity, or availability. Risk assessments should take into account the potential adverse impact on the University's reputation, operations, and assets. Risk assessments should include backups and non-original sources ofePHI.
3. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to review and update risk assessments every three years, or more frequently in response to significant legislative, environmental or operational changes.
4. It is the responsibility of each UCCS Designated Health Care Component's Leadership to inform the UCCS HIPAA Privacy and Security Official(s) of the completion of all documented risk assessments within thirty (30) calendar days of their completion, and provide a copy upon request.

Implemented Procedures:

C. §164.308(a)(1)(ii)(B) - Risk Management (Required)

It is the responsibility of each UCCS Designated Health Care Component's Leadership, the UCCS Director of Campus Compliance / Privacy Officer, UCCS HIPAA Security Officer, and the Office of Information Technology to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.308(a).

Practices for Compliance

1. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to select appropriate controls, e.g. policies, procedures, technologies, to safeguard data relative to the sensitivity or criticality determined by the risk assessment, and document the party(ies) responsible for implementation of each recommended practice.

2. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to, where possible, incorporate these Standards and practices when evaluating and selecting new hardware and software.

Implemented Procedures:

D. §164.308(a)(1)(ii)(C) - Sanction Policy (Required)

It is the responsibility of each UCCS Designated Health Care Component's Leadership, the UCCS Director of Campus Compliance / Privacy Officer, UCCS HIPAA Security Officer, the Office of Information Technology, and the Human Resources Department to apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.

Practices for Compliance

1. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with Human Resources and College / Center Leadership to take disciplinary or other action in accordance with University personnel policies, bargaining agreements, and guidelines on workforce members who, during their employment, fail to comply with University policy and procedures, including information security policy and procedures.
2. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with Human Resources and College / Center Leadership to ensure that documentation of violations and application of HIPAA-related sanctions is maintained appropriately and retained for sixyears.
   a. HIPAA entities are responsible for informing Human Resources and/or Labor Relations when submitting documentation with this retention requirement.

Implemented Procedures:

E. §164.308(a)(1)(ii)(D) - Information system activity review (Required)

It is the responsibility of each UCCS Designated Health Care Component's Leadership as well as the UCCS HIPAA Security Officer to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

Practices for Compliance

1. It is the responsibility of each UCCS Designated Health Care Component's Leadership or designee as well as the UCCS HIPAA Security Officer to regularly review information system activity and log-in attempts. The period for which activity logs are maintained and the extent, frequency, and nature of reviews are determined by the UCCS Designated Health Care Component's security environment and overall security management process. The UCCS Security Officer will determine the period of review at least annually.
2. It is the responsibility of each UCCS Designated Health Care Component's Leadership or designee as well as the UCCS HIPAA Security Officer to maintain documentation of periodic log reviews.

3. Logs relevant to security incidents should be retained for six years and the remainder of the data should only be retained for up to 90 days in accordance with usual and customary practice.
4. It is the responsibility of each UCCS Designated Health Care Component's Leadership as well as the UCCS HIPAA Security Officer to define responsibility for information system activity review, including log-in monitoring and access reports.

Implemented Procedures:

II. STANDARD

A. §164.308(a)(2) - Assigned security responsibility

It is the responsibility of each UCCS Designated Health Care Component's Leadership to identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.

Implemented Procedures:

III. STANDARD

A. §164.308(a)(3)(i) - Workforce security

It is the responsibility of each UCCS Designated Health Care Component's Leadership as well as the UCCS HIPAA Security Officer, and the Office of Information Technology to implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a) (4) of this section, and to prevent those workforce members who do not have access under paragraph (a) (4) of this section from obtaining access to electronic protected health information.

B. §164.308(a)(3)(ii)(A) - Authorization and/or supervision (Addressable)

It is the responsibility of each UCCS Designated Health Care Component's Leadership as well as the UCCS HIPAA Security Officer to implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

Practices for Compliance

1. It is the responsibility of each UCCS Designated Health Care Component's Leadership to determine which individuals are authorized to work with ePHI in accordance with a role-based approach.

Implemented Procedures:

C. §164.308(a)(3)(ii)(B) - Workforce clearance procedure (Addressable)

It is the responsibility of each UCCS Designated Health Care Component's Leadership as well as the UCCS HIPAA Security Officer to implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

Practices for Compliance

1. It is the responsibility of each UCCS Designated Health Care Component's Leadership, or designee, to review role definitions and assignments for appropriateness at least annually.
2. It is the responsibility of each UCCS Designated Health Care Components Leadership, or designee, to review access management procedures for appropriateness at least annually.

Implemented Procedures:

D. §164.308(a)(3)(ii)(C) - Termination procedures (Addressable)

It is the responsibility of each UCCS Designated Health Care Component's Leadership as well as the UCCS Office of Information Technology in conjunction with the Human Resources Department to implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a) (3) (ii) (B) of this section.

Practices for Compliance

1. It is the responsibility of each UCCS Designated Health Care Component's Leadership as well as the UCCS HIPAA Security Officer to establish account maintenance procedures that ensure termination of accounts or change in access privileges for individuals who have been terminated or are no longer authorized to access ePHI.

Implemented Procedures:

IV. STANDARD

A. §164.308(a)(4)(i) - Information access management

It is the responsibility of each UCCS Designated Health Care Component's Leadership as well as the UCCS HIPAA Security Officer to implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.

B. §164.308(a)(4)(ii)(A) - Isolating health care clearinghouse functions (Required)

If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.

Implemented Procedures:

C. §164.308(a)(4)(ii)(B) - Access authorization (Addressable)

It is the responsibility of each UCCS Designated Health Care Component's Leadership to implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

Practices for Compliance

1. It is the responsibility of each UCCS Designated Health Care Component's Leadership as well as the UCCS HIPAA Security Officer to ensure there is a formal system for authorizing user access to ePHI, such as an account request form requiring management approval.
2. It is the responsibility of each UCCS Designated Health Care Component's Leadership to ensure access is to be granted in accordance with a role-based approach.
3. It is the responsibility of each UCCS Designated Health Care Component's Leadership to maintain documentation of all authorized users of ePHI and their access levels.
4. It is the responsibility of each UCCS Designated Health Care Component's Leadership to ensure workforce members must receive security awareness and HIPAA training prior to obtaining access to ePHI.
5. It is the responsibility of each UCCS Designated Health Care Component's Leadership as well as the UCCS HIPAA Security Officer to ensure HIPAA systems must have the capacity to set accesscontrols.

Implemented Procedures:

D. §164.308(a)(4)(ii)(C) - Access establishment and modification (Addressable)

It is the responsibility of each UCCS Designated Health Care Component's Leadership as well as the UCCS HIPAA Security Officer to implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

Practices for Compliance

1. It is the responsibility of each UCCS Designated Health Care Component's Leadership as well as the UCCS HIPAA Security Officer and the UCCS Office of Information technology to develop and implement procedures to establish, document, review and modify a user's access to ePHI. Access shall use the principle of "least privileges."
2. It is the responsibility of each UCCS Designated Health Care Component's Leadership as well as the UCCS HIPAA Security Officer to ensure procedures include a regular review of those with access to ePHI, including the appropriateness of access levels. The period for which and the extent, frequency, and nature of reviews are determined by the UCCS Designated Health Care Component's security environment and overall security management process. The UCCS Security Officer will determine the period of review at least annually.
3. It is the responsibility of each UCCS Designated Health Care Component's Leadership as well as the UCCS HIPAA Security Officer and the UCCS Office of Information Technology to ensure procedures must require prompt initiation of account modifications/termination.

Implemented Procedures:

V. STANDARD

A. §164.308(a)(5)(i) - Security awareness and training

It is the responsibility of each UCCS Designated Health Care Component's Leadership as well as the UCCS Director of Campus Compliance / HIPAA Privacy Office and the HIPAA Security Officer to implement a security awareness and training program for all members of its workforce (including management).

B. §164.308(a)(5)(ii)(A) - Security reminders (Addressable)

It is the responsibility of each UCCS Designated Health Care Component's Leadership as well as the UCCS HIPAA Security Officer to ensure periodic security updates.

Practices for Compliance

1. It is the responsibility of each UCCS Designated Health Care Component's Leadership as well as the UCCS HIPAA Security Officer to establish security awareness and HIPAA training for all members of the UCCS workforce who are involved in the creation, transmission, and storage of ePHI. Training activities include:
   a. Initial security awareness and HIPAA training for individuals with ePHI-related job duties. Training will include UCCS Password Standards and the importance of protecting against malicious software and exploitation of vulnerabilities.
   b. Review of changes to internal policies, procedures, and technologies
   c. Periodic reminders about security awareness and HIPAA
   d. Security notices or updates regarding current threats
2. It is the responsibility of each UCCS Designated Health Care Component's Leadership as well as the UCCS HIPAA Security Officer to ensure HIPAA entities must maintain records of training materials and completion of training for six years.

Implemented Procedures:

C. §164.308(a)(5)(ii)(B) - Protection from malicious software (Addressable)

It is the responsibility of the UCCS HIPPA Security Officer in conjunction with the UCCS Information Technology Department to develop procedures for guarding against, detecting, and reporting malicious software.

Practices for Compliance

1. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the UCCS Information Technology Department to protect all devices against malicious software, such as computer viruses, Trojan horses, spyware, etc.,. Also ensure the safeguards and appropriate configurations are included in the standard set-up procedures for new systems and workstations that contain or access ePHI.
2. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the UCCS Information Technology Department to run versions of operating system and application software for which security patches are made available and installed in a timely manner in accordance with UCCS Security Standards for Information Systems. The UCCS Security Officer will determine the period of review at least annually.
3. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the UCCS Information Technology Department to harden systems. "Hardening" includes:
   a. Install OS and third-party application updates (patches) and keep them current
   b. Change or remove default logins/passwords
   c. Disable unnecessary services

d. Install virus and malware protection software and update them at least weekly
e. Set proper file/directory ownership/permissions;

4. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the UCCS Information Technology Department to periodically, and at least annually, review HIPAA workstation browser settings to ensure that they comply with UCCS Security Standards for Information Systems and UCCS Policy 700-002 Responsible Computing Section II.B.1.a.
5. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the UCCS Information Technology Department to periodically, and at least annually, review email client settings to ensure they comply with current UCCS Office of Information Technology recommendations.
6. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the UCCS Information Technology Department to perform periodic network vulnerability scans of systems containing known ePHI, and workstations that access ePHI, and take adequate steps to correct discovered vulnerabilities.
7. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the UCCS Information Technology Department to implement e-mail malicious code filtering.
8. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the UCCS Information Technology Department to install/enable firewalls (hardware and/or software) to reduce threat of unauthorized remote access.
9. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the UCCS Information Technology Department to ensure intrusion detection software and/or systems may also be installed to detect threat of unauthorized remote access.

Implemented Procedures:

D. §164.308(a)(5)(ii)(C) - Log-in monitoring (Addressable)

It is the responsibility of each UCCS Designated Health Care Component's Leadership as well as the UCCS HIPAA Security Officer to ensure procedures for monitoring log-in attempts and reporting discrepancies.

Practices for Compliance

See *§164.308(a)(1)(ii)(D) - Information system activity review,* above.

Implemented Procedures:

E. §164.308(a)(5)(ii)(D) - Password management (Addressable)

It is the responsibility of each UCCS Designated Health Care Component's Leadership as well as the UCCS HIPAA Security Officer in conjunction with the UCCS Office of Information Technology to develop procedures for creating, changing, and safeguarding passwords.

Practices for Compliance

1. Passwords for systems containing or accessing ePHI will comply with the UCCS Password Strength and Security Standards.

2. It is the responsibility of each UCCS Designated Health Care Component's Leadership to enforce UCCS password complexity requirements for third-party access as possible.

Implemented Procedures:

VI. STANDARD

A. §164.308(a)(6)(i) - Security incident procedures

It is the responsibility of each UCCS Designated Health Care Component's Leadership as well as the UCCS HIPAA Security Officer in conjunction with UCCS Office of Information Technology Department to implement policies and procedures to address security incidents.

B. §164.308(a)(6)(ii) - Response and Reporting (Required)

It is the responsibility of each UCCS Designated Health Care Component's Leadership as well as the UCCS HIPAA Security Officer in conjunction with UCCS Office of Information Technology Department to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the UCCS Designated Health Care Component; and document security incidents and their outcomes.

Practices for Compliance

1. Suspected or known security incidents involving ePHI must be reported to the campus HIPAA Security Officer. (Note: Privacy incidents involving ePHI must be reported to the UCCS Director of Campus Compliance / HIPAA Privacy Officer.) See *§164.308(a)(2) - Assigned security responsibility*, above.
2. It is the responsibility of each UCCS Designated Health Care Component's Leadership to have procedures and training in place to ensure that suspected or known security incidents involving ePHI are reported and documented appropriately as per Attachment 2 Documentation Policy (Retention).
3. Security incidents determined to involve ePHI must be documented, tracked and reported as defined in HIPAA entity documentation and UCCS Guidelines for Reporting Information Security Incidents.

Implemented Procedures:
Follow the incident response and reporting as described in the IT Security Website. Report immediately to HIPAA Office and HIPAA Security Officer.

VII. STANDARD

A. §164.308(a)(7)(i) - Contingency plan

It is the responsibility of each UCCS Designated Health Care Component's Leadership as well as the UCCS HIPAA Security Officer in conjunction with UCCS Office of Information Technology Department to establish (and implement as needed) policies and procedures for responding an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

B. §164.308(a)(7)(ii)(A) - Data backup plan (Required)

It is the responsibility of each UCCS Designated Health Care Component's Leadership as well as the UCCS

HIPAA Security Officer in conjunction with UCCS Office of Information Technology Department to establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

Practices for Compliance

1. It is the responsibility of each UCCS Designated Health Care Component's Leadership to ensure back up original sources of essential ePHI on an established schedule.
2. It is the responsibility of each UCCS Designated Health Care Component's Leadership to ensure backup copies are securely stored in a physically separate location from the data source.
3. It is the responsibility of each UCCS Designated Health Care Component's Leadership to ensure backups containing ePHI will be transported via secure methods.
4. It is the responsibility of each UCCS Designated Health Care Component's Leadership to ensure documentation exists to verify the creation of backups and their secure storage.

Implemented Procedures:

C. §164.308(a)(7)(ii)(B) - Disaster recovery plan (Required)

It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to establish (and implement as needed) procedures to restore any loss of data.

Practices for Compliance

1. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to establish procedures to restore loss of essential ePHI as a result of a disaster or emergency.
2. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to maintain copies of the data restoration procedures that are readily accessible at more than one location and should not rely on the availability of local power or network.
3. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to develop backup procedures that must include steps to ensure that all protections (patches, configurations, permissions, firewalls, etc.) are re-applied and restored before ePHI is restored to a system.

Implemented Procedures:

D. §164.308(a)(7)(ii)(C) - Emergency mode operation plan (Required)

It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

Practices for Compliance

1. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to ensure that HIPAA entity emergency operations procedures maintain security protections for ePHI.

2. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to evaluate operations in emergency mode, e.g. a technical failure or power outage, to determine whether security processes to protect ePHI are maintained.
3. It is the responsibility of each UCCS Designated Health Care Component's Leadership to document assessment and conclusions.
4. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to document and implement additional authorities and procedures necessary to ensure the continuation of security protections for ePHI during emergency operations mode.
5. It is the responsibility of each UCCS Designated Health Care Component's Leadership to develop plans for evacuations:
   a. UCCS Designated Health Care Component's entities' emergency response plans shall include logging out of systems that contain ePHI, securing files, and locking up before evacuating a building, if safe to do so.
   b. UCCS Designated Health Care Components should have processes to ensure there was no breach when the area is re-occupied.

Implemented Procedures:

E. §164.308(a)(7)(ii)(D) - Testing and revision procedures (Addressable)

It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to implement procedures for periodic testing and revision of contingency plans.

Practices for Compliance

1. It is the responsibility of each UCCS Designated Health Care Component's Leadership to document the contingency plan procedures.
2. It is the responsibility of each UCCS Designated Health Care Component's Leadership to ensure that those responsible for executing contingency plan procedures understand their responsibilities.
3. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to periodically, and at least annually, perform a test of the contingency plan procedures.
4. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to document test results, review and correct any problems with the test, and update procedures accordingly.

Implemented Procedures:

F. §164.308(a)(7)(ii)(E) - Applications and data criticality analysis (Addressable)

It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to assess the relative criticality of specific applications and data in support of other contingency plan components.

Practices for Compliance

1. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to prioritize criticality of applications and data sets for data back-up, restoration, and application of emergency mode operation plan.
2. Priorities can be included in data restoration procedures (*§164.308(a)(7)(ii)(B) - Disaster recovery plan*)

Implemented Procedures:

VIII. STANDARD

A. §164.308(a)(8) - Evaluation

It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.

Practices for Compliance

1. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer and the UCCS Director of Campus Compliance / HIPAA Privacy Officer to review and update campus HIPAA Policy and Practices for Compliance every five (5) years, or more frequently in response to environmental or operational changes that affect the security of ePHI.
   a. Submit to the UCCS HIPAA Security Officer and the UCCS Director of Campus Compliance / HIPAA Privacy Officer once annually by calendar year-end a list of titles and last revision dates of the policies designed to meet HIPAA Security Rule requirements, and provide copies upon request.
2. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer and the UCCS Director of Campus Compliance / HIPAA Privacy Officer to review and update Unit policies and procedures annually if there is no trigger for more frequent review.
3. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer and the UCCS Director of Campus Compliance / HIPAA Privacy Officer to identify the individual(s) responsible for determining when evaluation is necessary due to environmental or operational changes.
4. Document periodic reviews the updates and archive previous versions. Retain for six years as per Attachment 2 Documentation Policy (Retention).

Implemented Procedures:

IX. STANDARD

A. §164.308(b)(1) - Business associate contracts and other arrangements

A covered entity, in accordance with §164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the

covered entity obtains satisfactory assurances, in accordance with §164.314(a) that the business associate will appropriately safeguard the information.

B. §164.308(b)(4) - Written contract or other arrangement (Required)

It is the responsibility of each UCCS Designated Health Care Component's Leadership to document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a).

Practices for Compliance

1. It is the responsibility of each UCCS Designated Health Care Component's Leadership to ensure that agreements with business associates [1] contain language stating that University ePHI receives appropriate safeguards in accordance with Federal HIPAA Security Regulations.
2. It is the responsibility of each UCCS Designated Health Care Component's Leadership to use the UCCS Business Associate Agreements (BAA) template or send the third parties BAA to both UCCS Legal Counsel and Director of Campus Compliance / HIPAA Privacy Officer for review prior to signing.
3. It is the responsibility of each UCCS Designated Health Care Component's Leadership to ensure that UCCS-approved BAAs are in place at either a System-wide or local level for vendors and third-party service providers with access to UCCS ePHI or to systems that contain or access ePHI.
4. HIPAA entity procedures must include notifying Procurement Services when a HIPAA BAA is needed and when renewing an agreement with an existing HIPAA BAA.

Implemented Procedures:

HIPAA Security Rule: PHYSICAL STANDARDS

X. STANDARD

A. §164.310(a)(1) - Facility access controls

It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

B. §164.310(a)(2)(i) - Contingency Operations (Addressable)

It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

Practices for Compliance

[1] A "business associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or as a service to, a covered entity. This includes services where disclosure of ePHI is not limited in nature, such as destruction services or a software vendor that needs access to ePHI in order to provide its service. Common exclusions include health care providers that must comply with HIPAA requirements, conduits (physical or electronic) that transport but do not access protected health information, custodial services, destruction services when the work is performed under the direct control of the covered entity (in which case the service may be treated as part of the workforce). For additional clarification, inclusions and exclusions, see http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html and http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf, page 8378, column 1, (b)(1).

1. It is the responsibility of each UCCS Designated Health Care Component's Leadership to ensure that contingency procedures and authorization (See *§164.308(a)(7)(i): Administrative Standards – Contingency Plan*) include facility access.

Implemented Procedures:

C. §164.310(a)(2)(ii) - Facility security plan (Addressable)

It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer, UCCS Director of Campus Compliance / HIPAA Privacy Officer, and UCCS Facilities Services to implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

Practices for Compliance

1. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to ensure systems and electronic media containing ePHI are to be located in physically secure locations. A secure location would minimally be defined as one that is not routinely accessible to the public, particularly if authorized personnel are not always available to monitor security.
2. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS Facilities Services to ensure that secure locations have physical access controls (card key, door locks, alarms, etc.) that prevent unauthorized entry, particularly during periods outside of normal work hours, or when authorized personnel are not present to monitor security. If logging is available, it should be enabled.
3. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to ensure access control systems are maintained in good working order.
4. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with Facilities Services to ensure the facility security plans document use of physical access controls.

Implemented Procedures:

D. §164.310(a)(2)(iii) - Access control and validation procedures (Addressable)

It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer and the UCCS Director of Campus Compliance / HIPAA Privacy Officer to implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

Practices for Compliance

1. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to develop an access plan for facilities containing ePHI that utilizes role- or function-based access control, including for visitors, service providers, and contractors.

2. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to ensure the role- or function-based access control and validation procedures are closely aligned with the facility security plan.
3. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to ensure the security plan for facilities containing ePHI includes key systems or electronic door access.
5. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer, the UCCS Director of Campus Compliance / HIPAA Privacy Officer, UCCS Facility Services, and Human Resources to conduct a periodic (at least annual) review and implementation of termination procedures, which may include a review of key inventory or electronic door access, to ensure currency of access authorization.

Implemented Procedures:

§164.310(a)(2)(iv) - Maintenance records (Addressable)

It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS Facility Services Department to implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

Practices for Compliance

1. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS Facility Services Department to develop policy and procedure for maintaining a record of any maintenance repairs and modifications to physical components of a facility containing ePHI related to security, such as hardware, walls, doors, and locks.
   a. Documentation should contain appropriate detail for review, including date, repair, and/or modification(s) made, and the contractor.
   b. Documentation should be stored securely.
2. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS Facility Services Department to identify party(ies) responsible for recording and maintaining these records.

Implemented Procedures:

XI. STANDARD

A. §164.310(b) - Workstation use

It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI.

Practices for Compliance

1. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to ensure functions to be performed on workstations containing or accessing ePHI are aligned with roles.
2. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to develop policies and procedures that specify where to place and position workstations to only allow viewing by authorized individuals, as well as additional privacy measures, commensurate with the risk of exposure.
3. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to ensure unencrypted ePHI will not be stored on portable electronic devices, including laptops.
4. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to ensure storage of ePHI on non-university equipment is forbidden, except in the case of storage by a third party with a HIPAA BAA.
6. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer and the UCCS Office of Information Technology to ensure remote access of ePHI will utilize secure channels.

Implemented Procedures:

XII. STANDARD

A. §164.310(c) - Workstation security

It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

Practices for Compliance

1. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to ensure all workstations, including laptops, containing ePHI are to be physically secured (locked down).
2. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to ensure all workstations and electronic devices that contain or access ePHI will be identified, such as laptops, desktop computers, and personal digital assistants (PDAs).
3. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to ensure unencrypted ePHI will not be stored on portable electronic devices, including laptops.
4. If ePHI is stored on removable media, additional physical controls must be implemented, such as ensuring that the device is physically secured or in the physical possession of the responsible party. Encryption is a compensating control for these additional measures.

Implemented Procedures:

XIII. STANDARD

A. §164.310(d)(1) - Device and media controls

It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility.

B. §164.310(d)(2)(i) - Disposal (Required)

It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to implement policies and procedures to address the final disposition of ePHI, and/or the hardware or electronic media on which it is stored.

Practices for Compliance

1. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to ensure that ePHI on hardware and electronic media, including copiers, faxes, printers, etc., is unusable and/or inaccessible prior to disposal, including disposal by a Business Associate[2].
2. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to follow UCCS Policy 700-006 Computer and Electronics Disposal.
3. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to ensure when portable media is discarded, it must either be overwritten in accordance with National Institute of Standards and Technology (NIST) guidelines, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf, or physically destroyed, eliminating all possibility that any ePHI contents could be read.
4. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to ensure when a system is recycled, transferred to another user not authorized for the data, or discarded, all storage devices or all ePHI records must be overwritten in accordance with NIST guidelines (link above), or physically destroyed, rendering all ePHI records unreadable.

Implemented Procedures:

C. §164.310(d)(2)(ii) - Media re-use (Required)

It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to implement procedures for removal of ePHI from electronic media before the media are made available for re-use.

Practices for Compliance

1. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to ensure that ePHI on hardware and electronic media is unusable and/or inaccessible prior to re-use.
3. When a system is recycled or transferred to another user not authorized for the data, or otherwise re-used outside of a HIPAA-compliant environment, all storage devices or all ePHI records must be overwritten in accordance with National Institute of Standards and Technology (NIST) guidelines, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf, rendering all ePHI records unreadable.

[2] Also see §164.308(b)(1), Business associate contracts and other arrangements

Implemented Procedures:

D. §164.310(d)(2)(iii) - Accountability (Addressable)

It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to maintain a record of the movements of hardware and electronic media and any person responsible therefore.

Practices for Compliance

1. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to maintain a record of the movements of, and person(s) responsible for, hardware and electronic media containing ePHI.
    a. Identify all types of hardware and electronic media that must be tracked.
        i. Special attention must be paid to portable devices and removable media. These devices should not ordinarily contain ePHI and must be individually identified in the tracking system in order to contain ePHI. Their use must be consistent with the individual's identified role, such as according to a role-based matrix.
        ii. This inventory should be physically confirmed at least annually.
    b. Tracking system must include a mechanism for documenting the initial assignment of responsibility for devices that contain ePHI, as well as the transfer of authority for thesedevices.
2. Transport of archival media between the origination point and remote storage location must usea secure method to avoid unauthorized access to the archival media.
3. Loss or theft of electronic equipment or media containing ePHI must immediately be reported according to campus incident response procedures. https://www.uccs.edu/oit/security/incident-response. Also see *§164.308(a)(6)(i) - Security incident procedures*.

Implemented Procedures:

E. §164.310(d)(2)(iv) - Data backup and storage (Addressable)

It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to create a retrievable, exact copy of ePHI, when needed, before movement of equipment.

Practices for Compliance

1. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to create a retrievable, exact copy of original sources of essential ePHI before moving equipment containing them.
2. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to establish a process for documenting or verifying creation of retrievable, exact copy of original sources of essential ePHI.
4. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to develop retrievable, exact copies of ePHI that must be protected in accordance with these Standards.

Implemented Procedures:

HIPAA Security Rule: TECHNICAL STANDARDS

XIV. STANDARD

A. §164.312(a)(1) - Access Control

It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)

B. §164.312(a)(2)(i) - Unique user identification (Required)

It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to assign a unique name and/or number for identifying and tracking user identity.

Practices for Compliance

1. Each User must be provided a unique account, with a unique username/user ID and password, for access to ePHI.
2. Generic or shared accounts are not permitted for access to ePHI.

Implemented Procedures:

C. §164.312(a)(2)(ii) - Emergency access procedure (Required)

It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.

Practices for Compliance

1. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to establish procedures to ensure that necessary ePHI can be accessed during an emergency.
   a. Emergency access procedures may be included in Contingency Plan procedures (see *§164.308(a)(7)(i) - Contingency plan)*.
2. It is the responsibility of each UCCS Designated Health Care Component's Leadership in conjunction with the UCCS HIPAA Security Officer to develop emergency access procedures that shall be written and communicated in advance to multiple individuals within the organization.
3. It is the responsibility of each UCCS Designated Health Care Component's Leadership to ensure emergency access procedures should not rely on the availability of a single individual.
4. It is the responsibility of each UCCS Designated Health Care Component's Leadership to ensure access to emergency procedures should not rely on the availability of local power or network.
5. It is the responsibility of each UCCS Designated Health Care Component's Leadership to identify roles that may require special access during an emergency.
   a. Individuals are to require proper ID or other official verification before granting access to unknown or not-normally-authorized individuals in emergency circumstances.

Implemented Procedures:

D. §164.312(a)(2)(iii) - Automatic logoff (Addressable)

It is the responsibility of the UCCS HIPAA Security Officer in conjunction with each UCCS Designated Health Care Component's Leadership to implement electronic procedures that terminate an electronic session after a predetermined time of inactivity as per section XIV.D.3 below.

Practices for Compliance

1. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with each UCCS Designated Health Care Component's Leadership to ensure where possible, that electronic sessions terminate after a period of inactivity.
2. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with each UCCS Designated Health Care Component's Leadership to ensure, where session termination is not possible, either technically or from a business process perspective, automatic workstation lockout is implemented as a compensating control.
3. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with each UCCS Designated Health Care Component's Leadership to ensure a maximum duration of inactivity prior to session termination or automatic workstation lockout is 10 minutes. *Note: The UCCS Information Security Office may consider written requests for exceptions to the 10-minute requirement. These requests will be kept on file for 6 years.*

Implemented Procedures:

E. §164.312(a)(2)(iv) - Encryption and decryption (Addressable)

It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology to implement a mechanism to encrypt and decrypt ePHI.

Practices for Compliance

1. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology to implement appropriate security measures, such as encryption, to protect ePHI from unauthorized access.
   a. Unencrypted ePHI will not be stored on portable electronic devices, including laptops (see §164.310(b) - Workstation use and §164.310(c) - Workstation security).
2. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology to, in situations where encryption is problematic, implement the alternative compensating controls below as appropriate.
   a. It is the responsibility of the UCCS HIPAA Security Officer to keep an explanation for why encryption is not being implemented.
   b. Alternative, reasonable and appropriate compensating controls if encryption is not in place for stored ePHI:
      i. Access controls, including unique user ID & password authentication, and user profiles
      ii. Hardening of systems (see §164.308(a)(5)(ii)(B) - for details)
      iii. Physical security for access to facilities and workstations that contain or access ePHI, including appropriate device and media controls
      iv. Technically enforce complex passwords where possible
      v. Enable system security auditing/logging, including monitoring of audit reports/logs
      vi. Correct configuration of applications to use secure protocols
      vii. Implement automatic logoff and/or screen lock (see §164.312(a)(2)(iii) - for details)
      viii. Ensure secure remote access
      ix. Implement correctly configured firewalls (hardware and/or software)

Implemented Procedures:

XV. STANDARD

A. §164.312(b) - Audit controls

It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology, and if necessary each UCCS Designated Health Care Component's Leadership, to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

Practices for Compliance

1. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology, and if necessary each UCCS Designated Health Care Component's Leadership, to establish criteria for log creation, retention, and examination of activity.
2. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology, and if necessary each UCCS Designated Health Care Component's Leadership, to review that new systems should be selected with the ability to support audit requirements.
3. See §164.308(a)(1)(ii)(D) - Information system activity review for additional administrative practices.

Implemented Procedures:

XVI. STANDARD

A. §164.312(c)(1) – Integrity

It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology, and if necessary each UCCS Designated Health Care Component's Leadership, to implement policies and procedures to protect ePHI from improper alteration or destruction.

B. §164.312(c)(2) - Mechanism to authenticate electronic protected health information (Addressable)

It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology, and if necessary each UCCS Designated Health Care Component's Leadership, to implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.

Practices for Compliance

1. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology, and if necessary each UCCS Designated Health Care Component's Leadership, to leverage application-specific mechanisms or functionality when available to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.
2. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology, and if necessary each UCCS Designated Health Care Component's Leadership, to regularly review access logs for unauthorized direct access or administrator/root access to table data containing ePHI. The frequency at which activity logs are reviewed and the extent, frequency, and nature of reviews are determined by the UCCS Designated Health Care Component's security environment and overall security management process.
3. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology, and if necessary each UCCS Designated Health Care Component's

Leadership, to implement the following practices as a means of protecting ePHI from being altered or destroyed in an unauthorized manner:

a. Ensure appropriate physical security is in place for devices that contain or access ePHI (see *Physical Security Standards*).
b. Protect all devices against malicious software (see *§164.308(a)(5)(ii)(B) - Protection from malicious software* for details).
c. Protect sensitive data with appropriate strategies, such as secure file transfer *(§164.312(e)(1) - Transmission security*) and use of web browser security standards *(§164.308(a)(5)(ii)(B)) - Protection from malicious software*).
d. Implement processes to notify users and take other appropriate remedial action in the event of propagation of malicious software (see *§164.308(a)(5)(ii)(A) - Security reminders*).

Implemented Procedures:

XVII. STANDARD

A. §164.312(d) - Person or entity authentication

It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology, and if necessary each UCCS Designated Health Care Component's Leadership, to implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

Practices for Compliance

1. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology, and if necessary each UCCS Designated Health Care Component's Leadership, to ensure each User must be provided a unique account, with a unique User Name/ID and Password, for access to ePHI.
   a. Generic or shared accounts are not permitted for access to ePHI.
   b. Passwords for access to ePHI will not be shared by UCCS Employees or Workforce Members.
   c. All passwords providing access to ePHI, including local administrator/root passwords, must comply with the UCCS Policy 700-002 on Responsible Computing.
   d. Physically protect passwords
2. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology, and if necessary each UCCS Designated Health Care Component's Leadership, to review, as appropriate, workstation, OS and application access logs, as well as failed or successful changes to account permissions (*also see §164.308(a)(1)(ii)(D) - Information system activity review*).
3. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology, and if necessary each UCCS Designated Health Care Component's Leadership, to ensure systems and applications will not be configured to save passwords.
4. All of the above practices apply to vendors and third parties.

Implemented Procedures:

XVIII. STANDARD

A. 164.312(e)(1) - Transmission security

It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology, and if necessary each UCCS Designated Health Care Component's Leadership, to implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.

B. §164.312(e)(2)(i) - Integrity controls (Addressable)

It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology, and if necessary each UCCS Designated Health Care Component's Leadership, to implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.

Practices for Compliance

1. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology, and if necessary each UCCS Designated Health Care Component's Leadership, to ensure wired and wireless transmission of ePHI will use secureprotocols (encryption).
2. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology, and if necessary each UCCS Designated Health Care Component's Leadership, to ensure all remote access of ePHI must be by secure methods only.
3. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology, and if necessary each UCCS Designated Health Care Component's Leadership, to ensure unprotected ePHI shall not be sent via unencrypted email.
   a. Note: It is acceptable to send ePHI via email in encrypted, password-protected attachments to known business partners, and in response to legitimate requests if no secure channelexists.
4. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology, and if necessary each UCCS Designated Health Care Component's Leadership, to ensure received email containing ePHI is adequately deleted when there is no longer a business need to retain it. Procedures are available in individual HIPAA entity training or as requested of the OIT helpdesk.
5. UCCS Workforce Members must delete or redact ePHI from the body of received email before replying to it.

Implemented Procedures:

C. §164.312(e)(2)(ii) – Encryption (Addressable)

It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology, and if necessary each UCCS Designated Health Care Component's Leadership, to implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

See *§164.312(e)(2)(i) - Integrity controls (Addressable)*, above, for recommended practices.
Note: Also see *§164.312(a)(2)(iv) – Encryption and decryption (Addressable)*, above, for storage of ePHI.

Implemented Procedures: