University Policy 2202: Privacy and Security of Protected Health Information under HIPAA

Category: Community Expectations
Sub Category: Records Management & Privacy
Covered Individuals: University employees, students, and visitors
Responsible Executive: Office of Legal Affairs
Policy Custodian: Privacy Officer
Last Revised: 2024/11/08
Previous USU Policy Number: USU Policy 538, USU Policy 541

2202.1 PURPOSE AND SCOPE

The purpose of this Policy and related procedures is to provide a framework for Utah State University's compliance with the provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and other regulations for the privacy and security of Protected Health Information (PHI). The regulations associated with HIPAA require healthcare providers, health plans, and healthcare clearinghouses (referred to in HIPAA as Covered Entities) to provide privacy and security protections for PHI when they are engaged in certain activities (referred to as Covered Functions).

USU is a Covered Entity based on functions it carries out that qualify as Covered Functions. This policy applies to PHI created, acquired, or maintained by all staff, faculty, health care providers, volunteers, and consultants engaged in designated Health Care Components (HCCs) within USU and by contractors, subcontractors, vendors, and other entities acting as Business Associates to USU HCCs.

2202.2 POLICY

2.1 Utah State University HIPAA Component Designation

Units within Utah State University that provide Covered Functions or that share PHI with those units are "Health Care Components" (HCCs) as defined in 45 CFR, Part 160.103 and are known collectively as "USU Health Care Components." USU's Privacy Officer recommends to USU's HIPAA Steering Committee units that should be designated as HCCs, and the Steering Committee ratifies such recommendations. Departments, divisions, units, and functions designated as part of the USU HIPAA Health Care Components are listed in 2105-D2 USU HIPAA Hybrid Covered Entity Declaration in accordance with 45 CFR 164.105(c)(1).

In addition, anyone who believes that a department or program creates, uses, or discloses PHI and should be designated as part of USU's HIPAA Health Care Components should contact the University Privacy Officer.

2.2 The Privacy Rule

The HIPAA Privacy Rule limits the University's use and disclosure of information that could potentially associate an individual's identity with their health information. The University may not use or disclose PHI except as authorized by the individual, as permitted or required by law.

Use or disclosure of health information that does not have the potential to reveal an individual's identity (e.g., all HIPAA-designated identifiers have been removed from the data) is not limited under HIPAA. However, privacy or security issues, such as protecting research participants, may extend to Personally Identifiable Data not covered under HIPAA.

USU HCCs will make reasonable efforts to limit requests, uses, and disclosures involving PHI to the minimum required for the purpose at hand, as set forth in Procedure 2202-PR1, "Minimum Necessary Use and Disclosure of PHI at USU," and as may be further detailed in HCC-specific procedures and/or guidance as allowed under Section 2.5, below.

USU HCCs recognize the rights provided to individuals under 45 CFR 164.520 to receive adequate notice of the HCC's uses and disclosures of their PHI, as well as their privacy rights and the HCC's obligations with respect to their PHI. Notices are developed following 2202-PR5, "Patient Rights and Notifications to Patients and Patient Representatives," which follows requirements in 45 CFR 164.520(b). Notices describe:

- How the HCC may use and disclose PHI about the individual;
- The individual's rights with respect to the PHI and how the individual may exercise these rights, including how the individual may complain to the HCC;
- The HCC's legal duties with respect to the PHI, including a statement that the HCC is required by law to maintain the privacy of PHI;
- Whom individuals can contact for further information about the covered entity's privacy policies.

The notice must include an effective date. HCCs are required to promptly revise and distribute privacy notices whenever material changes are made to privacy practices within the HCC. Effective notice must be made available to any person who asks for it, and notices must be prominently posted and made available on any website the HCC maintains.

USU's health plan HCCs must provide notice of privacy practices to enrollees at the time of enrollment. Health Plan Notices of Privacy Practices follow regulations provided in 45 CFR 164, sections 520(b)(3) and 520(c)(1)(i)(C).

The HIPAA Privacy Rule is distinguished from the HIPAA Security Rule in that the security regulation applies to electronic storage and transmission of PHI (ePHI), compared with the privacy regulation, which applies to all forms of PHI and prescribes more detailed requirements for securing such data.

2.3 The Security Rule

To protect the confidentiality, integrity, and availability of electronically Protected Health Information (ePHI) created, received, maintained, or transmitted by USU HCCs, each HCC shall meet or exceed standards set in the HIPAA Security Rule. The standards include implementing appropriate and reasonable administrative, physical, and technical security measures sufficient to reduce risks and vulnerabilities. Such measures shall be implemented based on the level of risks, capabilities, and operating requirements of each HCC.

For additional information, refer to Procedure 2202-PR2, "Provision of Safeguards Applicable to Protected Health Information," available on USU's HIPAA website.

2.4 Group Health Plan

As an employer, Utah State University offers various health plans to its employees and retirees, which comprise the Group Health Plan. Some of the medical plans are funded by the University ("Self-Funded" group health plans), and others are fully insured by an insurance carrier ("Funded" or fully insured group health plans). The University's Self-Funded Plans and the Health Flexible Spending Account are covered components that collectively form the USU Health Plan Component (UHPC).

Governance of uses and disclosures of PHI by the Group Health Plan, including the UHPC, shall be as set forth in Procedure 2202-PR4, "HIPAA Uses and Disclosures for USU Group Health Plans."

2.5 Unit-Specific Guidance and Procedures

Each USU HCC shall comply with University policies as well as develop, implement, document, and train its workforce on procedures necessary to comply with HIPAA requirements and with this Policy. For information regarding specific HCC procedures, workforce members should contact the HCC privacy and/or security delegate or the unit supervisor.

HCCs will comply with requests by USU's Privacy Officer, Security Officer, or others in the Office of Legal Affairs or USU's Internal Audit Services to make written procedures and training material available for internal review.

2.6 Research Using Health Information

In the course of research, university employees who are not affiliated with USU HCCs under USU's HIPAA Hybrid Entity Declaration may obtain, create, use and/or disclose individually identifiable health information. Such research data is protected under 45 CFR 46.111. The privacy of participants in Human Subjects Research and the confidentiality of related information is overseen by USU's IRB.

Under the Privacy Rule, individuals affiliated with covered components of the university who are obtaining or creating individually identifiable health information while engaged in activities within the covered component may use such information for research purposes as set forth in Procedure 2202-PR1, "Minimum Necessary Use and Disclosure of PHI at USU," available at usu.edu/compliance.

Clinician-researchers must exercise care to avoid using or disclosing PHI obtained or created in an incident to provide clinical services not allowed under HIPAA and/or the Common Rule, except as authorized or allowed under the Privacy Rule.

2.7 Business Associates

Contractors and/or vendors that have access to PHI while providing certain services, functions, or activities for an HCC at USU must enter into a Business Associate Agreement (BAA) governing the use, maintenance, and disclosure of PHI. The agreement shall set forth appropriate safeguards for the PHI it receives or creates on behalf of the covered entity. When possible, HCCs shall use the HIPAA Business Associate Agreement Template, available at USU's HIPAA website.

2.8 Training

USU HCCs will coordinate with the Office of Data Governance to establish ongoing security awareness through training or other means that provide their workforce with procedure updates concerning both privacy and security practices. New members of the workforce for whom HIPAA training is necessary or appropriate will be trained prior to initial contact with PHI and in no event later than 30 days from the first

date of employment. Each member of the workforce whose functions are affected by a material change in the policies or procedures will be trained on those changes promptly, but normally not later than 30 working days from the effective date of the change. HCCs will document that workforce training has been completed and will retain these records in the format requested by the University Privacy Officer and/ or the Information Security Officer.

2.9 Violations

Anyone who knows or has reason to believe that the Privacy Rule and/or the Security Rule, the University HIPAA policies and procedures, or USU HCC procedures have been violated should report the matter promptly to his or her supervisor, a USU HCC official, the University Privacy Officer, or the Information Security Officer, where appropriate. All reported matters will be investigated promptly and, when possible, handled confidentially.

If a workforce member requires anonymity, they may also report such matters using the USU Reporting Hotline System, located at https://www.usu.edu/compliance/reporting/how-to, or by calling (844) 916-2760.

To the extent practicable, any known harmful effect from a violation of the Privacy Rule or the Security Rule or a security incident will be mitigated. Where appropriate, sanctions will be considered and imposed by USU. USU HCCs should document all investigations, resolutions, remedies, and sanctions in accordance with USU Procedure 2202-PR3 for Implementation of Corrective Actions Involving Violations of Individual's Privacy or Security and forward a copy of such documentation to the University Privacy Officer or Information Security Officer, as appropriate.

Sanctions resulting from violations by individuals of the Privacy Rule or Security Rule may, under certain circumstances, result in civil or criminal penalties. Members of the workforce who violate the Privacy Rule, Security Rule, USU policies, or procedures implementing these policies may also be subject to disciplinary action up to and including termination of employment, contract, or other relationship with USU.

2.10 Breach Notification Rule

The Breach Notification Rule, 45 CFR §§ 164.400-414, requires USU HCCs and their Business Associates to provide notification following a breach of unsecured protected health information. In the event of a breach, USU will notify affected individuals, the Secretary of HHS, and, where applicable, the media in accordance with prescribed notification procedures as set forth in Procedure 2105-PR6, "Breach Notification for Unsecured PHI."

2.11 Refraining from Intimidation or Retaliatory Attacks

Personnel at USU HCCs will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any patient, physician, clinician, employee, or any other person for exercising his or her rights or for participating in any process established under the Privacy Rule or Security Rule, including submitting a complaint or reporting a violation in accordance with Section 2.9 above. Any attempt to retaliate against a person for reporting a violation in accordance with this Section 2.11 may itself be considered a violation of this policy and may result in disciplinary action.

An individual who raises concerns about any act or practice allegedly made unlawfully by the Privacy Rule or Security Rule, however, must have a good faith belief that the act or practice is unlawful, and the manner of raising such concerns must be reasonable and not violate the Privacy Rule or Security Rule.

Individuals will not be required to waive any of their rights, including the right to file a complaint under the

HIPAA regulations as a condition of treatment, payment, enrollment in a health plan, or establishing eligibility for benefits.

2.12 Evaluation and Reporting

Each USU HCC will provide the University Privacy Officer and/or the Information Security Officer with all requested information in order to adequately address complaints, respond to requests, and inform leadership about compliance with the Privacy Rule or Security Rule.

2.13 Documentation and Retention

All policies, procedures, communications, actions, activities, and/or designations that require documentation under HIPAA shall be maintained in written and/or electronic form and retained for a period not less than seven years from the final action recorded or 22 years after the date of birth, whichever is later. Retention of documents beyond this required minimum shall be in accordance with any Federal or additional State requirement with respect to each document.

2202.3 RESPONSIBILITIES

3.1 Privacy Officials

Within the Office of Legal Affairs, USU has designated a HIPAA Privacy Officer responsible for privacy issues across the university, including compliance with the Privacy Rule in HIPAA, 45 CFR Parts 160. The HIPAA Privacy Officer is responsible for coordinating the development and implementation of procedures necessary to comply with HIPAA at the university level and within the HCCs.

The University Privacy Officer works with HCC-designated privacy officers as necessary to effectively implement the policies and procedures within their programs. The USU HIPAA Privacy Officer and HCC-specific privacy officers will act promptly to ensure compliance with all regulations and Steering Committee directives.

3.2. Security Officials

Utah State University has designated a HIPAA Security Officer responsible for HIPAA-related information security issues throughout the university, including compliance with the Security Rule as contained in 45 CFR 162 & 164. The HIPAA Security Officer is responsible for coordinating the development of procedures necessary to comply with the Security Rule and implementing security measures to protect electronic Protected Health Information (ePHI).

The Data Privacy Office works in conjunction with the HIPAA Security Officer, HCC-designated and other unit-designated security officers, colleges, departments, or other units to accomplish broad data security objectives as outlined in the Data Security Policy and to implement policies, procedures, and other measures related to data security.

3.3 HIPAA Steering Committee

USU has created a standing steering committee to oversee HIPAA activities across the university. It has specific responsibility for ratifying the inclusion of USU units that carry out Covered Functions as HCCs in the Hybrid Entity Declaration and for regular reviews of the Hybrid Entity Declaration, this policy and associated guidance, procedures, and training programs designed to support the security, maintenance, transfer, use, and disclosure of PHI at USU. It also considers the inclusion - as part of USU's HCCs - of certain personnel or units that, if they were separate entities, would be considered

Business Associates.

3.4 Employees of HCCs

Employees within the Health Care Components of the university may use or disclose PHI only when the action is part of the employee's duties. Such uses or disclosures must follow the principles outlined in Procedure 2202-PR1 on "Minimum Necessary Use and Disclosure of PHI at USU." Individuals at USU clinics may occasionally authorize the use or disclosure of their PHI for purposes such as research. Such authorizations do not alter the employee's responsibilities to protect the confidentiality of PHI except to the extent the employee has explicit responsibility for carrying out the disclosure or use specified in the written authorization. Unauthorized use or disclosure of PHI may result in disciplinary action by USU and may expose the employee to criminal prosecution. PHI that resides within USU facilities and/or systems shall not be removed from the university or transferred via unencrypted mobile devices or through unencrypted electronic transfers.

3.5 USU Employees

Employees of USU may occasionally have access to personal information through the receipt of limited data sets or as a function of their duties, such as enrolling university personnel in health plans. Any employee with access to any PHI or Personally Identifiable Information (PII) is expected to maintain the confidentiality of that information and use it only to complete assigned duties at USU. Any employee who unexpectedly receives PHI or PII must report the incident to his/her direct supervisor immediately or to the Privacy Officer if the supervisor is not available. The disclosure of such information may constitute a breach, which may be subject to reporting requirements by USU. All employees of USU HCCs must receive HIPAA training in accordance with 2.8 above.

3.6 USU Students

Students at USU sometimes participate in internships, externships, or other similar placements in organizations and agencies that are covered entities under HIPAA. During such placements, students may be considered members of the covered entity's workforce. Such students must receive training concerning the Privacy and Security Rules under HIPAA, available at USU through departments and through USU's Institutional Learning System, and, where appropriate, must be provided with training concerning the policies and procedures related to HIPAA at the receiving organization.

2202.4 REFERENCES

- 45 CFR Part 160, HIPAA General Administrative Requirements
- 45 CFR Part 162, HIPAA Administrative Requirements
- 45 CFR 164, HIPAA Security and Privacy, as amended

2202.5 RELATED USU POLICIES

- Privacy (Pending)
- Data Security (Pending)
- 2101.5 Non-retaliation (included in Policy 2101: Discrimination based on Protected Characteristics)

Information below is not included as part of the contents of the official policy. It is provided only as a convenience for readers/users and may be changed at any time by persons authorized by the president.

RESOURCES

Procedures

2202-PR1: Minimum Necessary Use and Disclosure of PHI
2202-PR2: Provision of Safeguards Applicable to Protected Health Information (PHI)
2202-PR3: Implementation of Corrective Actions Involving Violations of Individual's Privacy or Security
2202-PR4: HIPAA Uses and Disclosures for USU Group Health Plans
2202-PR5: Patient Rights and Notifications to Patients and Patient Representatives
2202-PR6: Breach Notifications for Unsecured PHI
2202-PR7: Business Associate Relationships with Vendors
SCCE Supplemental Privacy Policies

Related Forms and Tools

- Business Associate Agreement Template
- Breach Assessment

Contacts

- HIPAA Privacy Officer
  (435) 797-8305

- HIPAA Security Officer
  (435) 797-8305

POLICY HISTORY

Original issue date: 2020/12/09

Last review date: 2024/11/08

Next scheduled review date: 2027/10/1

Previous Revision Dates:

- **2020/12/09:** Originally issued as USU Policy 538 (previously also assigned as Policy 540).
- **2022/12/09:** Originally issued as USU Policy 541, designated as USU Policy 547. This revision added the following procedures to the policy:
  - 547-PR5: Patient Rights and Notifications to Patients and Patient Representatives
  - 547-PR6: Breach Notifications for Unsecured PHI
  - 547-PR7: Business Associate Relationships with Vendors
  - SCCE Supplemental Privacy Policies