UH HIPAA Policy

J. T. Ash
University of Hawaii System
HIPAA Compliance Officer
jtash@hawaii.edu
hipaa@hawaii.edu

Agenda

- HIPAA is a "**TEAM SPORT**" and everyone has a role in protecting protected health information (PHI).
- Purpose of the UH HIPAA Policy
- Objectives of the UH HIPAA Policy
- General Requirements and practices
- Roles and responsibilities
- Policies and procedures

UH HIPAA Policy Purpose

- Ensure that the University of Hawai‘i (the “University”) complies with the Health Insurance Portability and Accountability Act of 1996, as amended by the American Recovery and Reinvestment Act of 2009 (“ARRA”), which included the Health Information Technology for Economic and Clinical Health Act (“HITECH”) that expanded the scope of privacy and security protections, and by the implementing regulations at 45 Code of Federal Regulations (“CFR”) Parts 160, 162 and 164, as amended (collectively referred to as “HIPAA”).

UH HIPAA Policy Objectives

- Establish University System-wide policies and procedures to:
  - Designate the University as a Hybrid Entity
  - Establish fundamental principles governing the University's management and use of Protected Health Information ("PHI")
  - Establish a set of standardized terms and definitions to promote consistent interpretation and implementation of the University's HIPAA Policy.
  - Establish clear lines of authority and accountability related to PHI.
  - Set forth best practices for HIPAA compliance with the ongoing objectives of:
    - Identifying University units and subunits (and their activities) that are subject to HIPAA
    - Managing and mitigating information privacy and security risks related to PHI.

General requirements and practices

- DO NOT share PHI with the non-covered Units of the University (See Below)
- Comply with HIPAA and this HIPAA Policy
- Perform a risk assessment
- Designate a Unit HIPAA Coordinator
- Complete HIPAA training
- Maintain a BAA with another internal University Unit or an entity outside the University to share PHI or a Limited Data Set.
- Maintain a Data Use Agreement and BAA that receives the Limited Data Set, and such use has been approved by the University's Institutional Review Board ("IRB").
- Posts a Notice of Privacy Practices as required by HIPAA

Roles and responsibilities – Office of the Vice President for Information Technology and Chief Information Officer (OVPIT)

- Designate staff to serve as the University System HIPAA Privacy and Security Officer(s)

Roles and responsibilities – UH System HIPAA Privacy and Security Officer

- **Relating to the HIPAA Privacy Rule:**

- Maintain ongoing communication with all Unit HIPAA Coordinators;

- Coordinate training programs for the designated UH Covered Components (employees, students and volunteers) in cooperation with the Unit HIPAA Coordinators

- Maintain ongoing communications with the IRB regarding research use of PHI and Limited Data Sets

- Respond to complaints regarding University policies, procedures and practices related to the privacy of health information

- Respond, or refer, to the appropriate UH Covered Component, requests by individuals for access and amendment, an accounting of disclosures, or requested restrictions to the use and disclosure of PHI.

- Approve and execute all BAAs, Data Use Agreements, and Data Sharing Agreements.

Roles and responsibilities – UH System HIPAA Privacy and Security Officer

- **Relating to the HIPAA Security Rule:**

- Maintain ongoing communication with the Unit HIPAA Coordinators;

- Guide and assist with the development and implementation of ongoing security awareness and training programs for the employees, students, and volunteers of each UH Covered Component

- Monitor the use of security measures to protect PHI

- Assist in revising this HIPAA Policy and any University policy or procedure related to the privacy and security of PHI, as required to comply with changes in any applicable law, as well as documenting any change to any policy or procedure related to the privacy and security of PHI.

Roles and responsibilities – Unit HIPAA Coordinators

- Maintain ongoing communication with the UH System HIPAA Privacy and Security Officer(s)
- Develop and maintain procedures consistent with this HIPAA Policy for protection of PHI and ePHI in the University Unit, which is considered a UH Covered Component
- Maintain and update, as needed, procedures consistent with the policy for protection of PHI and ePHI in the University Unit
- Inform employees, volunteers, students, and as needed, consultants and others, about this HIPAA Policy and all University policies and procedures relating to HIPAA through various methods including but not limited to staff meetings, in person meetings, seminars, orientation meetings and phone or web based meetings
- Monitor the process of identifying and training new employees, volunteers and students within the University Unit who require access to PHI
- Monitor compliance with the policies and procedures of the University Unit relating to HIPAA

Roles and responsibilities – Unit HIPAA Coordinators

- Report directly to the UH System HIPAA Privacy and Security Officer(s), any and all violations that result in an impermissible use or disclosure of PHI and/or ePHI;
- Report directly to the UH System HIPAA Privacy and Security Officer(s), any and all privacy violations under HIPAA;
- Report directly to the UH System HIPAA Privacy and Security Officer(s), any and all security violations under HIPAA;
- Ensure continued compliance with HIPAA, this HIPAA Policy, and all University policies and procedures relating to HIPAA; and
- Review all BAAs, Data Use and Data Sharing Agreements prior to execution by the Project Principal Investigator or Program Lead.

Policies and procedures

- General Requirements and Practices:
  - Sharing PHI
  - Risk Assessment
  - Designate a Coordinator
  - HIPAA Training
  - BAA Management (Internal & External)

Policies and procedures – HIPAA Privacy

- **Relating to the HIPAA Privacy Rule:**
  - Disclosure only with consent
  - Disclosure required to individual and DHHS
  - Disclosure to UH Covered Component
  - Disclosure to Business Associate
  - Disclosure pursuant to valid authorization
  - Disclosure for marketing purposes
  - Disclosure of psychotherapy notes
  - Disclosure relating to minors
  - Disclosure requiring advance notice and opportunity to agree or object
  - Disclosure when authorization or opportunity to agree or object not required
  - Disclosure to determine identity or cause of death
  - Disclosure for research purposes

Policies and procedures – HIPAA Privacy (continued)

- Disclosure to prevent/lessen imminent threat of harm
- Disclosure for workers compensation purposes
- Disclosure of de-identified data
- Disclosure of Limited Data Set
- Disclosure consent requires prior notice of privacy practices
- Disclosure by Unit which is a federally assisted drug abuse program or a federally assisted alcohol abuse program
- Rights to request privacy protection for PHI
- Access of individuals to PHI
- Amendment of PHI
- Accounting of disclosures of PHI
- Administrative requirements
- Organizational Options (Covered Entities must designate in writing its operations that perform covered functions as one or more “health care components).

Policies and procedures – HIPAA Security

- Relating to the HIPAA Security Rule (**Administrative safeguards**)
  - Security Management Process § 164.308(a)(1)
    - Risk Analysis (R)
    - Risk Management (R)
    - Sanction Policy (R)
    - Information System Activity Review (R)
  - Assigned Security Responsibility § 164.308(a)(2)
  - Workforce Security § 164.308(a)(3)
    - Authorization and/or Supervision (A)
    - Workforce Clearance Procedure (A)
    - Termination Procedures (A)
  - Information Access Management § 164.308(a)(4)
    - Isolating Health Care Clearinghouse Functions (R)
    - Access Authorization (A)
    - Access Establishment and Modification (A)

Policies and procedures – HIPAA Security

- Relating to the HIPAA Security Rule (**Administrative safeguards**)
  - Security Awareness and Training § 164.308(a)(5)
    - Security Reminders (A)
    - Protection from Malicious Software (A)
    - Log-in Monitoring (A)
    - Password Management (A)
  - Security Incident Procedures § 164.308(a)(6)
    - Response and Reporting (R)
  - Contingency Plan § 164.308(a)(7)
    - Data Backup Plan (R)
    - Disaster Recovery Plan (R)
    - Emergency Mode Operation Plan (R)
    - Testing and Revision Procedures (A)
    - Applications and Data Criticality Analysis (A)

Policies and procedures – HIPAA Security

- Relating to the HIPAA Security Rule (**Administrative safeguards**)
  - Evaluation § 164.308(a)(8)
  - Business Associate Contracts and § 164.308(b)(1)
    - Written Contract or Other Arrangement (R)
  - Other Arrangements

Policies and procedures – HIPAA Security

- Relating to the HIPAA Security Rule (**Physical safeguards**)
  - Facility Access Controls § 164.310(a)(1)
    - Contingency Operations (A)
    - Facility Security Plan (A)
    - Access Control and Validation Procedures (A)
    - Maintenance Records (A)
  - Workstation Use § 164.310(b)
  - Workstation Security § 164.310(c)
  - Device and Media Controls § 164.310(d)(1)
    - Disposal (R)
    - Media Re-use (R)
    - Accountability (A)
    - Data Backup and Storage (A)

Policies and procedures – HIPAA Security

- Relating to the HIPAA Security Rule (**Technical safeguards**)
  - Access Control § 164.312(a)(1)
    - Unique User Identification (R)
    - Emergency Access Procedure (R)
    - Automatic Logoff (A)
    - Encryption and Decryption (A)
  - Audit Control § 164.312(b)
  - Integrity § 164.312(c)(1)
    - Mechanism to Authenticate Electronic Protected Health Information (A)
  - Person or Entity Authentication § 164.312(d)
  - Transmission Security § 164.312(e)(1)
    - Encryption (A)
    - Integrity Controls (A)

Policies and procedures – HIPAA Security

- Relating to the HIPAA Security Rule (**Breach of Unsecured PHI**)
  - Notification in the Case of Breach of Unsecured PHI
  - Notification to Individuals
  - Notification to others
  - Notification to the DHHS Secretary
  - Notification by a Business Associate
  - Notification to and coordination with UH System HIPAA Privacy and Security Officer(s)

J. T. Ash
UH System HIPAA Compliance Officer
jtash@hawaii.edu • (808) 956-7241