HIPAA PRIVACY
in an
ACADEMIC ENVIRONMENT

Mildred L. Johnson, J.D., CPC, CHC
Compliance Director, Baylor College of Medicine*

Colleen Shannon
Chief Compliance & Privacy Officer
Duke University Health System

Mildred Johnson
Compliance Director
Baylor College of Medicine
The views expressed here are those of the speakers and do not necessarily represent the views of their respective institutions.

Foundation

- The HIPAA Privacy rules require a Covered Entity to establish policies & procedures to ensure the confidentiality of PHI. 45 CFR 164.530(i)

- An effective compliance program requires:
  - Establishing an on-going monitoring/auditing program.
  - Investigation and remediation of Non-compliance
Investigation: Learners

- Who are “Learners”? 
  - Students and Residents 
    - Who employs the Resident – Hospital, School, Other?

- Affiliate Relationship Considerations 
  - Hospitals v. Community Physician Offices 
  - Whose PHI is involved? 
  - Who will conduct the investigation?

Investigation: Learners

- Investigation Considerations 
  - Pre-Investigation Notifications 
  - Conducting the investigation? 
  - Validation of Breach Determination 
    - Who will Report to OCR?; Who will provide Notice?

- Corrective Action Considerations 
  - Education of Peers; Publication 
  - Institutional Authority over the individual
Interfaces – Source of Truth

- Identification of All Data Interfaces
  - Whose Data controls?
  - Hospital, Diagnostic, Other?
- Electronic Controls to validate “matches” before an “overwrite”
  - Impact
    - Weak or Strong?
  - Process to work potential matches

Monitoring Program

- Develop a Written Procedure outlining
  - Responsibility
  - Areas to Monitor
    - Access (Internal and External)
    - Business Operations
    - Research Activities (Preparatory; IRB approved)
  - Frequency
  - Response to identified areas of improvement
  - Reporting
Access: External Partners

- Who are your External Partners?
  - Consultants
  - Affiliates (Hospitals; Coders; Quality; Case Managers – ACO/MACRA)
  - Non-Affiliate clinical “partners”
- Is there a Business Associate Agreement?
  - Is Access consistent with the stated purposes?
  - Is it the minimum necessary?

Access: External Partners

- Controls – Written Agreement
  - Coordinate Process with IT/EHR Staff
  - Determine Access Level: View v. Writing
    - If they are writing – are there billing implications?
  - Monitoring Responsibilities
    - Who, When, What, How
  - Notification Responsibilities
    - Termination/Position Change – Timeliness (especially with cloud based EHRs).
Internal Access Monitoring

- EHR “Access” Controls (e.g., Break the Glass)
  - Understand how the control is set up
    - User v. Department v. Patient
    - Timing Parameters
    - Other
  - EHR Reports and/or Third-party vendor programs
    - Internal Reporting limited to data within the EHR
    - External programs – what other data resources (e.g., HR) to interface to enhance monitoring activity.

Internal Access: Considerations

- EHR Controls
  - Validation of Compliant Use (e.g., Is a Reason or Explanation Required?)
  - “False” Positives
    - HIM; Schedulers; Quality; Coders; IT
    - Family Members (?)
      - Common last names; Same address, but multi-family units (apartments).
    - Researchers - validate against documentation
  - Volume – Is it feasible to evaluate all accesses?
Monitoring: Access Termination

- Written Policies setting forth
  - Timing
    - Impact of Cloud-based databases
    - Accountable parties
  - Was access terminated within stated timeframes
    - Employees
      - Voluntary v. Involuntary Terminations
    - Contractors and Others

Site Visits

- Where is Your PHI Used/Accessed/Disclosed
  - Clinical Areas; Business Units; Research Areas
- Develop Checklist
  - Posting & Delivery of Privacy Notice (Clinical Areas)
  - Faxing Procedures
  - Security of electronic and paper PHI
  - Staff knowledge of key Privacy/Security areas
- Coordination with Departments/Clinical Areas
- Opportunities
Site Visits

- Reporting
  - Department/Area Admin/Leader
    - Preliminary to allow opportunity to provide feedback and provide corrective action plan
    - Schedule follow-up to confirm implementation of any corrective action plan.
  - Leadership/Compliance Committee
    - Identify number of areas visited during the reporting period
    - Quantify common problem areas and corrective action implemented.

Other Monitoring Areas

- Patient Portals
  - Validation of “proxy” access documentation
- Release of Information/HIM
  - Timeliness
  - Accuracy & Completeness of Releases
- Research Access
  - Learners; Coordinators; Research Personnel
- Health Information Exchanges
Foundation

Privacy Rule minimum necessary requirements:

- Covered Entity is to make reasonable efforts:
  - to limit use and disclosure of PHI to the minimum necessary for intended purpose. 45 CFR 164.502(b)
  - to limit unnecessary/inappropriate access to PHI through access and policies and procedures. 45 CFR 164.514(d)
    - Access is based on job function. Covered Entity is required to determine workforce members who need access to PHI, PHI categories and conditions appropriate to such access.

Sharing Data

- Increased Requests for Access to EHRs for Predictive Analytics/machine learning to improve clinical outcomes
  - Clinical Research
  - Quality Improvement

- Requests include requests for large amount of data
## Sharing Data

**Considerations**
- Create secured, collaborative work space
- Access Protocols
  - Approved Research Protocol
  - Medical/Administrative Leadership approval of QI project
  - Data Use Agreements
- Minimum Necessary data sets
  - De-identified
  - Limited Data sets

## Sharing Data

**Develop data protocol**
- Centralized data resource to protect privacy and create consistency and accuracy of data
  - Access to dataset, not primary source
  - Delivery of datasets to work space
- Removal of data from work space
  - Creation of Honest Broker/Data Transfer
    - Verification of compliance with protocol
    - Minimum necessary protocol
Sharing Data

- Additional Considerations
  - Storage in Cloud
    - Establish internal protocols to secure transmission of data
    - Collaboration with cloud provider for audit trails

Segregation of Access for Multiple Roles

- Covered Entity must develop minimum necessary access to PHI.

- OCR: “A covered entity also is required to develop role-based access policies and procedures that limit which members of its workforce may have access to protected health information for treatment, payment, and health care operations, based on those who need access to the information to do their jobs.”
Segregation of Access for Multiple Roles

- To achieve role-based access, AMC must consider:
  - Control of data access
  - Separation by role
  - Auditing by responsibility
- Users must be given access only to PHI to perform role

Segregation of Access for Multiple Roles

- AMCs – staff have multiple roles:
  - Clinician vs. Research
  - Clinician vs. Student
  - Clinician vs. Scribe
  - Clinician vs. Administrator
  - Faculty vs. Fellow
- Each role requires different access and user rights
Segregation of Access for Multiple Roles

Considerations

- Create multiple role-based accesses/security templates
  - Staff responsible to log in based upon current performing role
  - Role-based access tied to author’s credentials
  - Role-based access limits security rights
    - Access certain portions of record, e.g., Medication Administration, Orders, Psych records
    - Edit record
    - Write orders

Segmentation of Access for Multiple Roles

Considerations

- Audit by role
  - Requires multiple audit views
  - Controls – review schedules, research protocols

- Role verification audits
  - Incorporate within transfer protocols
  - Incorporate within performance evaluation
  - Routine audits
### Segregation of Access for Multiple Roles

**Considerations**

- **Transfer/Termination of Roles**
  - Example -- Student access terminates upon end of rotation
  - Tie job code to role based access

- **Security Governance**
  - Centralized administration of security templates
  - Include Privacy, Compliance, Clinicians and Technical

### Foundation

**Privacy Rule Business Associate requirements:**

- Business Associate definition. 45 CFR 164.103
- Covered Entity may disclose PHI to a business associate who may create, receive, maintain, or transmit PHI, if the Covered Entity obtains satisfactory assurance to safeguard PHI. 45 CFR 164.502(e)(1)
- Security of data. 45 CFR 164.308-312, & 316
Managing BAAs

- OCR Phase 2 Audits require maintenance of business associate listing
  - Name, service provided, 2 contacts (address, phone, fax, email, website)
  - Process for updates

<table>
<thead>
<tr>
<th>BA Name</th>
<th>Type of Service Provided</th>
<th>POC1 Title</th>
<th>POC1 First Name</th>
<th>POC1 Last Name</th>
<th>POC1 Address</th>
<th>POC1 Address Contact</th>
<th>POC1 City</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNITED COUNSELING SERVICE OF REMINGTON COUNTY, INC.</td>
<td>HR Director</td>
<td>Amy</td>
<td>Felix</td>
<td>PO BOX 568</td>
<td>123 First St, City, State</td>
<td>REMINGTON</td>
<td></td>
</tr>
<tr>
<td>Association De Manos De Puerto Rico</td>
<td>President</td>
<td>Ana</td>
<td>Diego</td>
<td>EDU Prince St, City, State</td>
<td>San Juan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Idaho Department of Health, B.</td>
<td>Privacy Officer</td>
<td>Hugo</td>
<td>Graham</td>
<td>PO Box 45520</td>
<td>Boise</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/batemplate/index.html

Managing BAAs

- Considerations
  - Centralize BAA process
  - Revise service agreement/BAA include 2 notice contacts with contact information and obligations to provide updates
  - Contract Management Tool include BAA fields
    - OCR listing information
    - Create OCR report from fields
  - Routine review of BAA inventory
    - Review purchase orders
    - System interfaces/external party access
Managing BAAs

- Considerations
  - Verify services and BAA updated as vendor services change, e.g., additional products
    - BAA Appendix that is updated with new services/agreements
  - Manage Business Associates’ access to clinical systems
    - Provisioning process as own staff
    - Routine Exclusion screening
    - Routine access verification
      - Risk – employee termination triggers automatic termination of systems
      - Need separate process for vendors’ staff

- Additional Considerations
  - Data security agreements
  - Required third party audits of business associates’ processes
    - Cloud providers, EHR providers, database managers
    - Consultants often overlooked
  - Third party audits include: HITRUST, ISO, SOC
    - Independent party attestation of implementation of security, availability, integrity, and privacy of data
    - changes to Trust Services Criteria and SOC 2 Reports (12/18/2018)