When HHS Calls, Will Your Plan Be HIPAA-Compliant?

Petula Workman, J.D., CEBS
Division Vice President
Compliance Counsel
Gallagher Benefit Services, Inc.,
Sugar Land, Texas
HIPAA PRIVACY, SECURITY, AND BREACH AUDITS OVERVIEW
HIPAA Privacy, Security, and Breach Audits

• The Privacy and Security Regulations were passed as part of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”)
  – Amended by the HITECH Act

• The Privacy Regulations require “Covered Entities” and “Business Associates” to follow certain rules when handling and securing certain health information called “Protected Health Information” (or “PHI”)

• The Security Regulations establish a national set of security standards for protecting PHI held or transferred in electronic form

• The Breach Regulations address impermissible uses or disclosures under the Privacy Rule that compromise the security or privacy of PHI such that the use or disclosure poses a significant risk of financial, reputational, or other harm to an affected individual
HIPAA Privacy, Security, and Breach Audits

• “Covered Entities” are:
  – Health Plans
  – Health Care Clearinghouses
  – Health Care Providers
HIPAA Privacy, Security, and Breach Audits

- HITECH requires HHS to provide for periodic audits to ensure covered entities and business associates are complying with the HIPAA Privacy and Security Rules and Breach Notification standards
- OCR piloted a program to perform 115 audits of covered entities to assess privacy and security compliance (Phase I)
- Audits conducted during the pilot phase between November 2011 and December 2012
- New audit program for 2014 (Phase II)
HIPAA Privacy, Security, and Breach Audits

HIPAA Privacy & Security Rule Complaint Process

**Complaint**
- Possible Criminal Violation
  - DOJ declines case & refers back to OCR
- Possible Privacy or Security Rule Violation
  - Intake & Review

**Intake & Review**

**Investigation**

**Resolution**

- The violation did not occur after April 14, 2003
- Entity is not covered by the Privacy Rule
- Complaint was not filed within 180 days and an extension was not granted
- The incident described in the complaint does not violate the Privacy Rule

- OCR finds no violation
- OCR obtains voluntary compliance, corrective action, or other agreement
- OCR issues formal finding of violation

15A-6
Phase I Audits

- **1 Day**: Notification letter sent to Covered Entities
- **Minimum of 10 Days**: Receiving and Reviewing Documentation and Planning the Audit Field Work
- **3 – 10 Days**: Onsite fieldwork
- **20 – 30 Days**: Draft Audit Report
- **10 Days**: Covered Entities Review and Comment on Draft Audit Reports
- **30 Days**: Final Audit Report

Start Time: Day 1

Dependent on completion of fieldwork: Day 30/90
Phase II Audits

1. Notification and Data Request (two weeks to respond)
2. Desk audit with draft findings
3. Covered Entity provides management review of draft finding
4. Final Report
Phase II Audits

• New Audit Process
  – Primarily internally staffed
  – Covered entities will be asked to identify their business associates and provide current contact information
  – No on-site visits unless resources allow
  – No opportunity for investigator to seek additional information
  – Will use sampling methodology
Phase II Audits

- October 2014 through June 2015
  - 232 Providers
  - 109 Health Plans
  - 9 Clearinghouses
- OCR to use results of survey to select covered entities for audit
## Phase II Audits

<table>
<thead>
<tr>
<th>Entity Type</th>
<th>Privacy</th>
<th>Breach</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Covered Entities</strong></td>
<td>100</td>
<td>100</td>
<td>150</td>
</tr>
<tr>
<td>• Health Plans</td>
<td>33</td>
<td>31</td>
<td>45</td>
</tr>
<tr>
<td>• Providers</td>
<td>67</td>
<td>65</td>
<td>100</td>
</tr>
<tr>
<td>• Clearinghouses</td>
<td>0</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td><strong>Business Associates</strong></td>
<td>0</td>
<td>0</td>
<td>50</td>
</tr>
<tr>
<td>• IT Related</td>
<td>0</td>
<td>0</td>
<td>35</td>
</tr>
<tr>
<td>• Non-IT Related (e.g., TPAs, claims)</td>
<td>0</td>
<td>0</td>
<td>15</td>
</tr>
<tr>
<td><strong>Total Audits by Protocol</strong></td>
<td>100</td>
<td>100</td>
<td>200</td>
</tr>
</tbody>
</table>
HIPAA Privacy, Security, and Breach Audits

• Sampling of Documents Requested in Phase I
  – Demographics
  – Policies and procedures (Privacy, Security, and Breach)
  – Key person information
  – Organizational chart
  – Incident response plans
  – Risk assessment procedures
  – Contingency plans
  – System generated information (e.g., log files)
  – Technical controls information
  – Physical safeguards
  – Network diagrams
  – Notice of Privacy Practices
New HIPAA Regulations

- Omnibus regulations issued
  January 17, 2013
- Changes to
  - Notice of Privacy Practices
  - Policies and Procedures
    - Right to request restriction on use and disclosure
    - Right to access PHI
  - Breach Notification Rule
  - Business Associate Agreements
- GBS Technical Bulletin
  - [https://ajg.adobeconnect.com/_a815130238/tb_2013_01/](https://ajg.adobeconnect.com/_a815130238/tb_2013_01/)
Privacy
Privacy

• Administrative, Technical, and Physical safeguards
  – A covered entity must have reasonable safeguards to protect PHI from unintentional use or disclosure of PHI
  – Auditor will
    • Obtain and review written policies and procedures
    • Observe and verify that safeguards are in place and appropriate
Privacy

- Policies and Procedures
  - Maintaining and Updating Notice of Privacy Practices
  - Documentation of Compliance Activity
  - Limitations on Access
  - Mandatory Uses and Disclosures
  - Permissible Uses and Disclosures
  - Disclosures for Legal or Public Policy Reasons
  - Sanctions and Violations
  - Other Miscellaneous Policies
Privacy

• Mitigation
  – Covered entity must, to the extent practicable, mitigate any known harmful effect of a use or disclosure of PHI in violation of its own policies and procedures or the HIPAA regulations by itself or a business associate
  – Auditor will
    • Obtain and review policies and procedures
    • Determine if monitoring system is in place
    • Determine if policies and procedures are updated appropriately and communicated to workforce members
Privacy

• Refraining from intimidating or retaliatory acts
  – A covered entity may not intimidate, threaten, coerce, discriminate against, or take any other retaliatory action against an individual who exercises a HIPAA right or participates in the filing of a complaint either under the covered entity’s own policies and procedures or with HHS
  – Auditor will
    • Obtain and review policies and procedures
    • Determine whether policies and procedures are updated appropriately and communicated to workforce members
Security
Security

• The security rule covers the administrative, technical, and physical security measures entities are required to take with regard to maintenance and transmission of electronic PHI
• Some are “required” and some are “addressable”
• The security rule applies to all electronic PHI
  – Defined as PHI that is transmitted by, or maintained in, electronic media
    • Laptops
    • Mobile devices
    • USBs
    • CDs
    • Drives
    • Desktops
    • Tablets
    • Email
  – Does not apply to paper PHI
Security

• The security rule has five categories of requirements
  1. Administrative safeguards
  2. Physical safeguards
  3. Technical safeguards
  4. Organizational requirements
  5. Policies and procedures, and documentation
• Each category has a certain number of
  – “Standards”
  – Each standard has “implementation specifications”, which can be “required” or “addressable”
Security

• “Implementation Specification: Required”
  – Entities must comply with the implementation specification
  – Unless otherwise specified, entities have flexibility in determining how best to implement the specification
  • Must take into account
    – Size, complexity, and capabilities
    – Technical infrastructure, hardware, software security
    – Probability and criticality of potential risks of ePHI compromise
    – Cost of security measures
• “Implementation Specification: Addressable”
  – Entity must determine whether the implementation specification is a reasonable and appropriate safeguard
  – If not reasonable and appropriate, must document why it is not reasonable and appropriate
  – Entity must implement an alternative measure, again only if reasonable and appropriate
  – If an alternative measure is not implemented the entity must document why an alternative was not implemented and what measures are being done to ensure specification is being met
Security

• Assignment of Security Official (Required)
  – An entity must assign a security officer
  – Responsible for the development, implementation, monitoring, and communication of security policies and procedures
  – Must be a person, not a committee or group
Security

• Assignment of Security Official (Required)
  – Auditor will
    • Request information to demonstrate designation of Security Official
    • Obtain and review Security Official’s assigned duties
      – E.g., a job description
    • Determine if responsibilities have been clearly defined
Security

• Conduct periodic risk analysis (Required)
  – Must have policies and procedures to conduct an accurate assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI
  • Identify all assets and information systems that create, receive, transmit, or maintain ePHI
    – Assets: Computers, mobile devices, tablets, USB, etc.
    – Information systems: Software systems
Security

• Conduct periodic risk analysis (Required)
  – Auditor will review relevant documents and content to determine:
    • If periodic risk assessment conducted
    • Whether all assets and information systems that contain, process, or transmit ePHI have been identified
    • Whether risk assessment processes have been updated to reflect any changes in organizational environment
      – E.g., new email system, new servers
Security

• At the core of a risk analysis are the following questions:
  – Have you identified the e-PHI within your organization? This includes e-PHI that you create, receive, maintain or transmit.
  – What are the external sources of e-PHI? For example, do vendors or consultants create, receive, maintain or transmit e-PHI?
  – What are the human, natural, and environmental threats to information systems that contain e-PHI?
Security

• Development of policies and procedures for acquisition of IT Systems and Services (Required)
  – Must have processes in place for the selection of IT systems and services that include consideration for the following:
    • Applicability of the IT solution to the intended environment
    • The sensitivity of the data
    • The organization’s security policies, procedures, and standards
    • Other requirements such as resources available for operations, maintenance, and training
Security

• Development of policies and procedures for acquisition of IT Systems and Services (Required)
  – Auditor will
    • Review written policies and procedures for compliance
    • Determine whether policies and procedures are approved and updated on a periodic basis
• Information System Activity Review (Required)
  – Entity must implement procedures for regular reviewing of information system activity
    • Audit logs, access reports, security incident reports
    • Sign in/out reports, what reports were accessed, denied access or gained access
  – Timing is up to the entity
• Information System Activity Review (Required)
  – Auditor will
    • Review policies and procedures
    • Obtain sample of implementation of review practices (e.g., sample audit logs or access reports)
    • Determine if policies and procedures are approved and updated on periodic basis
Security

• Implementation of risk management program (Required)
  – Entity is required to implement proper security measures to reduce the risk of security threats
  – This is based on the risk analysis
Security

• Implementation of risk management program (Required)
  – Auditor will
    • Review security policies and evaluate whether security measures are sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with regulations
      – Vulnerability is defined as “[a] flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system’s security policy”
      – Risk is defined as “[t]he net mission impact considering (1) the probability that a particular [threat] will exercise (accidentally trigger or intentionally exploit) a particular [vulnerability] and (2) the resulting impact if this should occur . . .”
Security

• Implementation of risk management program (Required)
  – Auditor will
    • Determine if policy is reviewed and approved on a periodic basis
    • Determine if security standard addresses data moved within the organization and data sent out of the organization
Security

• Implementation of procedures for authorization and/or supervision of workforce members (Addressable)
  – Personnel accessing ePHI must be given authorization or be supervised
  – Up to the entity to determine best way to implement
  – Must address how to keep people who do not have access from inadvertent access
Security

- Implementation of policies and procedures to ensure appropriate access to ePHI by establishing clear job descriptions and responsibilities (Addressable)
  - Auditor will
    - Obtain and review formal documentation of policies and procedures to determine level of access granted based on business need
    - If entity has determined not to fully implement this standard, obtain documentation for areas without full implementation and rationale for not fully implementing
Security

• Implementation of policies and procedures to ensure appropriate access to ePHI by establishing criteria for hiring and assigning tasks (Addressable)
  – Process to determine whether a person should have access to ePHI
  – Assessment of risk, cost, benefit, and feasibility, and any other protective measures
Security

• Implementation of policies and procedures to ensure appropriate access to ePHI by establishing criteria for hiring and assigning tasks (Addressable)
  – Auditor will
    • Obtain and review documentation demonstrating that staff members have necessary knowledge, skills, and abilities to fulfill particular roles
    • Obtain and review documentation that management verified the required experience and qualifications per management policy
    • If entity has determined not to fully implement this standard, obtain documentation for areas without full implementation and rationale for not fully implementing
Security

• Establishment of Workforce Clearance (Addressable)
  – Process to determine whether a person should have access to ePHI
  – Assessment of risk, cost, benefit, and feasibility, and any other protective measures
Security

• Establishment of Workforce Clearance (Addressable)
  – Auditor will
  • Obtain and review policies and procedures
  • Obtain and review evidence of approval or verification of access to ePHI
  • If entity has determined not to fully implement this standard, obtain documentation for areas without full implementation and rationale for not fully implementing
Breach Notification
Breach Notification

• What is a “breach”?
  – An unauthorized acquisition, access, or use or disclosure of unsecured protected health information in a manner not permitted by the HIPAA Breach regulations which compromises the security or privacy of such information
    • “Unsecured” means that the information was not destroyed or otherwise rendered unusable (e.g., encrypted)
    • Not every disclosure is a breach
    • There are exceptions, but that is beyond the scope of our discussion today
Breach Notification

• Risk Assessment of Breach
  – Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Breach Notification regulations that compromises the security or privacy of the PHI
  – Auditor will
    • Ask if risk assessment process exists to determine whether breach exists
  – Should have written policies and procedures
Breach Notification

• Notice to Individuals
  – A covered entity is required to notify each impacted individual whose unsecured PHI has been or is reasonably believed to have been used, accessed, acquired, or disclosed as a result of a breach
  – Auditor will
    • Obtain and review key documents that outline the process for notifying individuals of breaches
  – Should have model forms to use to track investigation and notify individuals, HHS, and the media of breaches
• **Timeliness of Notification**
  
  – A covered entity is required to provide notice of a breach without unreasonable delay, but in no case later than 60 days after the discovery of the breach.
  
  – Auditor will
    
    • Obtain and review key documents that outline the process for notifying individuals.
    
    • Verify timing of breach notification, if any have occurred.
Breach Notification

• Methods of Individual Notification
  – Written notification is required, but if individual is deceased, notification may be given to next of kin or personal representative
  – Auditor will
    • Obtain and review documents that provide methods for notifying individuals and compare to actual performance
    • Request process to identify contact information or next of kin and the process to follow up if insufficient contact information
    • Obtain and review documents that provide methods to provide notice when contact information is insufficient or out-of-date
Breach Notification

• Content of Notification
  – Notification must contain
    • Brief description of what occurred
    • Date of breach
    • Date of discovery of breach (if known)
    • Description of unsecured PHI that was involved (e.g., Social Security number, diagnosis, etc.)
    • Steps individual should take to protect himself or herself from potential harm (e.g., notification of credit agencies)
    • Description of what covered entity is doing to investigate, mitigate harm, and protect against future potential breaches
    • Contact procedures for questions or additional information (e.g., toll free number to call)
• Content of Notification
  – Auditor will
    • Determine if any standard template or form letter used for breach notification
    • Verify notifications sent to individuals contained required elements, if any breaches occurred
Practice Pointers
Practice Pointers

• Audit Focus (Round 1)
  – Security
    • Risk analysis and risk management
  – Breach
    • Content and timeliness of notifications
  – Privacy
    • Notice and Access

• Audit Focus (Round 2) (Projected for 2015)
  – Security
    • Device and media controls, transmission security
  – Privacy
    • Safeguards, training to policies and procedures

• Audit Focus (Round 3) (Projected for 2016)
  – Security
    • Encryption and decryption; physical facility access control; other areas of high risk identified in 2014 audits; and breach reports and complaints
Practice Pointers

• Have pre-response strategy call with consultants
• Obtain advice of legal counsel when situation difficult
• Prepare documents in tabbed and labeled binders
• Consider vendor documents and procedures
• Prepare narrative responses in consultation with consultants and/or legal advisors
• Make sure that individuals required for interviews are available (if on-site visit occurs)
• Treat auditors with courtesy
HIPAA Privacy, Security and Breach Audits

• Resources
  – OCR Privacy & Security Audit webpage
    • http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html
  – OCR Privacy Assistance
    • http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/privacyguidance.html
  – OCR Security Assistance
    • http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html
The intent of this presentation is to provide you with general information regarding the topic presented. It does not necessarily fully address specific issues with respect to your employee benefits environment. It should not be construed as, nor is it intended to provide, legal advice. Questions regarding specific issues should be addressed by your general counsel or an attorney who specializes in this practice area.
## Policies and Procedures Audit Checklist for HIPAA Privacy, Security, and Breach Notification

<table>
<thead>
<tr>
<th>Type of Policy and Procedure</th>
<th>Comments</th>
<th>Completed</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Policy to Maintain and Update Notice of Privacy Practices</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notice of Privacy Practices</td>
<td>Health plans and covered health care providers are required to develop and distribute a notice that provides a clear explanation of privacy practices and an individual’s privacy rights. Develop policies and procedures.</td>
<td></td>
</tr>
<tr>
<td>Uses and disclosures consistent with Notice of Privacy Practices</td>
<td>Uses and disclosures of PHI must be in a manner that is consistent with Notice of Privacy Practices. Uses and disclosures must be outlined in Notice of Privacy Practices. Develop policies and procedures.</td>
<td></td>
</tr>
<tr>
<td><strong>Policy for Documentation of Compliance Activity</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Document retention</td>
<td>Policy and procedures for document retention should last a minimum of six years. Develop policies and procedures.</td>
<td></td>
</tr>
<tr>
<td><strong>Policy for Limitation on Access</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Workforce member training</td>
<td>A covered entity is required to train all members of its workforce on the policies and procedures related to PHI under HIPAA, as necessary and appropriate according to the function of each member’s position within the workforce. Develop policies, procedures, forms, and training.</td>
<td></td>
</tr>
<tr>
<td>Minimum Necessary Uses and Disclosures of PHI</td>
<td>The Plan and the organization shall take reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose when using or disclosing PHI or seeking PHI from another covered entity. Develop policies and procedures.</td>
<td></td>
</tr>
<tr>
<td>Use and disclosure of PHI by plan sponsor</td>
<td>Develop policies and procedures.</td>
<td></td>
</tr>
<tr>
<td>Type of Policy and Procedure</td>
<td>Comments</td>
<td>Completed</td>
</tr>
<tr>
<td>------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Policies for Handling Individual Rights</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidential communications</td>
<td>Individuals may request to receive PHI communications by alternative means or at alternative locations. Develop policies, procedures, and forms.</td>
<td></td>
</tr>
<tr>
<td>Right of individual to request restriction on use or disclosure of PHI</td>
<td>Individuals have a right to request restrictions on uses and disclosures of PHI about the individual to carry out treatment, payment and health care operations, and disclosures made to family members or persons who are involved in the health care of the individual. Develop policies, procedures, and forms.</td>
<td></td>
</tr>
<tr>
<td>Right of individual to access or amend own PHI</td>
<td>Individuals have the right to review or obtain copies of their own PHI. Individuals also have the right to request amendments to their PHI, with some exception. Develop policies, procedures, and forms.</td>
<td></td>
</tr>
<tr>
<td>Termination of restriction on use or disclosure of PHI</td>
<td>Develop policies, procedures, and forms.</td>
<td></td>
</tr>
<tr>
<td>Right of individual to amend PHI</td>
<td>Individuals have the right to amend or correct their PHI. Develop policies, procedures, and forms.</td>
<td></td>
</tr>
<tr>
<td>Right to request an accounting of disclosures</td>
<td>Individuals have the right to request an accounting of disclosures that are beyond certain parameters. Develop policies, procedures, and forms.</td>
<td></td>
</tr>
<tr>
<td>Policies and Procedures for Using and Disclosing PHI</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Uses and disclosures of PHI when individual is present</td>
<td>If the individual is present, the covered entity may use or disclose PHI if the covered entity obtains the individual’s consent, provides an opportunity to object, or determines there is no objection based on circumstances (e.g., with a translator). Develop policies and procedures.</td>
<td></td>
</tr>
<tr>
<td>Limitations on uses and disclosure of PHI when individual not present</td>
<td>If the individual is not present, the covered entity may determine whether the disclosure is in the best interests of the individual and, if so, disclose only the PHI that is directly relevant to the person’s involvement with the individual's care or payment related to the individual's healthcare or needed for notification purposes (e.g., individual is incapacitated). Develop policies and procedures.</td>
<td></td>
</tr>
<tr>
<td>Type of Policy and Procedure</td>
<td>Comments</td>
<td>Completed</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Determination as to whether authorization is valid</td>
<td>Develop policies and procedures.</td>
<td></td>
</tr>
<tr>
<td>Verification of individuals who request PHI</td>
<td>Develop policies and procedures for the verification of the identity of those requesting PHI. Include policies and procedures for: individual, spouse, domestic partner, civil union partner, parent seeking the PHI of a minor child, authorized personal representative, public officials, and person involved in individuals’ care. Develop policies and procedures.</td>
<td></td>
</tr>
<tr>
<td>Uses and disclosures of PHI to family members, relatives, close personal friends, or others authorized by individual (Personal Representatives)</td>
<td>Develop policies and procedures.</td>
<td></td>
</tr>
<tr>
<td>Terminating a restriction on the use or disclosure of PHI</td>
<td>Develop policies and procedures.</td>
<td></td>
</tr>
<tr>
<td>Uses and disclosures for underwriting and related purposes</td>
<td>A plan that performs underwriting (including but not limited to setting a plan’s premium, employee contributions or granting a premium reduction to an individual) may not use or disclose PHI that is genetic information for underwriting purposes, except in the case of long term care coverage. Develop policies and procedures.</td>
<td></td>
</tr>
<tr>
<td>Limited data sets and data use agreements</td>
<td>Ensure that data use agreements cover the use and disclosure of limited data sets. Although still PHI, a covered entity may use and disclose limited data sets. Develop policies and procedures.</td>
<td></td>
</tr>
<tr>
<td>Re-identification of PHI</td>
<td>Develop policies and procedures.</td>
<td></td>
</tr>
<tr>
<td>De-identification of PHI</td>
<td>De-identified Information is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. Policies and procedures for de-identifying PHI should include an explanation of identifiers. Develop policies and procedures.</td>
<td></td>
</tr>
<tr>
<td>Permitted uses and disclosures</td>
<td>Outline permitted uses and disclosures of PHI. Develop policies and procedures.</td>
<td></td>
</tr>
<tr>
<td>Type of Policy and Procedure</td>
<td>Comments</td>
<td>Completed</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Uses and disclosures pursuant to an authorization</td>
<td>Outline permitted uses and disclosures of PHI allowed pursuant to an authorization. Develop policies, procedures, and forms.</td>
<td></td>
</tr>
<tr>
<td>Deceased individuals</td>
<td>Plan may disclose PHI of a deceased person to family or other individuals involved in the person’s care prior to their death unless doing so is “inconsistent with any prior expressed preference” of the deceased, if known. Develop policies and procedures.</td>
<td></td>
</tr>
<tr>
<td>Personal Representatives</td>
<td>Personal Representative may request PHI on individual’s behalf. Individual must designate Personal Representative using “Designation of Personal Representative.” Policy and procedure should exist for verification of the identity of the Personal Representative requesting the PHI. Develop policies, procedures, and forms.</td>
<td></td>
</tr>
</tbody>
</table>

### Policies and Procedures for Disclosure for Legal or Public Policy Reasons

<table>
<thead>
<tr>
<th>Type of Policy and Procedure</th>
<th>Comments</th>
<th>Completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Whistleblowers</td>
<td>Whistleblowers are protected when disclosing PHI to oversight authorities. Develop policies and procedures.</td>
<td></td>
</tr>
<tr>
<td>Disclosures by workforce members who are victims of a crime</td>
<td>Disclosure of PHI in certain cases for victims of a crime. Develop policies and procedures.</td>
<td></td>
</tr>
<tr>
<td>Uses and disclosures of PHI for judicial and administrative proceedings</td>
<td>A health plan may disclose PHI for judicial and administrative proceedings with notice to the individual. Develop policies and procedures.</td>
<td></td>
</tr>
<tr>
<td>Uses and disclosures of PHI when required by law</td>
<td>Develop policies and procedures.</td>
<td></td>
</tr>
<tr>
<td>Uses and disclosures of PHI for public health activities</td>
<td>Develop policies and procedures.</td>
<td></td>
</tr>
<tr>
<td>Disclosures of PHI about victims of abuse, neglect, or domestic violence</td>
<td>Develop policies and procedures.</td>
<td></td>
</tr>
<tr>
<td>Disclosures for health oversight activities</td>
<td>Develop policies and procedures.</td>
<td></td>
</tr>
<tr>
<td>Disclosures for law enforcement purposes</td>
<td>Develop policies and procedures.</td>
<td></td>
</tr>
<tr>
<td>Type of Policy and Procedure</td>
<td>Comments</td>
<td>Completed</td>
</tr>
<tr>
<td>------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Uses and disclosures for cadaveric organ, eye or tissue</td>
<td>Develop policies and procedures.</td>
<td></td>
</tr>
<tr>
<td>Disclosures for Armed Forces activities</td>
<td>Develop policies and procedures.</td>
<td></td>
</tr>
<tr>
<td>Disclosures for prisoners</td>
<td>Develop policies and procedures.</td>
<td></td>
</tr>
<tr>
<td>Disclosures for workers’ compensation purposes</td>
<td>Develop policies and procedures.</td>
<td></td>
</tr>
<tr>
<td><strong>Miscellaneous Policies and Procedures</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prohibition on conditioning treatment, payment, or healthcare operations on provision of authorization</td>
<td>Develop policies and procedures.</td>
<td></td>
</tr>
<tr>
<td>Opportunity to object to use or disclosure</td>
<td>Develop policies, procedures, and forms.</td>
<td></td>
</tr>
<tr>
<td>Business Associate contracts</td>
<td>Develop policies, procedures, and model agreements outlining the handling and use of PHI by Business Associate.</td>
<td></td>
</tr>
<tr>
<td>Handling complaints</td>
<td>Complaints should be sent to, investigated, and tracked by the Privacy Officer. Develop policies, procedures, and forms.</td>
<td></td>
</tr>
<tr>
<td>Sanctions for violations</td>
<td>Must have sanctions against workforce members that violate privacy policies and procedures. Develop policies, procedures, and forms.</td>
<td></td>
</tr>
<tr>
<td>Mitigation of harm</td>
<td>Must, to extent practicable, mitigate any known harmful effect of a use or disclosure of PHI in violation of its own policies and procedures or of HIPAA regulations by its own workforce members or a business associate. Develop policies and procedures.</td>
<td></td>
</tr>
<tr>
<td>Refraining from intimidating or retaliatory acts</td>
<td>May not intimidate, threaten, coerce, discriminate against, or take any other retaliatory action against an individual who exercises a HIPAA right or participates in the filing of a complaint either under the covered entity’s own policies and procedures or with HHS. Develop policies and procedures. Include in training.</td>
<td></td>
</tr>
<tr>
<td>Type of Policy and Procedure</td>
<td>Comments</td>
<td>Completed</td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td><strong>Administrative, Technical, and Physical Safeguards</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reasonable safeguards to protect PHI from unintentional use or disclosure (Privacy)</td>
<td>Must have reasonable safeguards to protect PHI from unintentional use or disclosure of PHI. Develop policies and procedures.</td>
<td></td>
</tr>
<tr>
<td>Conducting periodic risk assessments (Security)</td>
<td>Must have policies and procedures to conduct an accurate assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI. Develop policies and procedures. Document measures.</td>
<td></td>
</tr>
<tr>
<td>Acquisition of IT Systems (Security)</td>
<td>Must have processes in place for the selection of IT systems and services. Develop policies and procedures. Document measures.</td>
<td></td>
</tr>
<tr>
<td>Information System Activity (Security)</td>
<td>Must have policies and procedures for regulating viewing of information system activity. Develop policies and procedures. Document measures.</td>
<td></td>
</tr>
<tr>
<td>Risk Management program (Security)</td>
<td>Must have property security measures in place to reduce the risk of security threats. Develop policies and procedures. Document measures.</td>
<td></td>
</tr>
<tr>
<td>Authorization and/or supervision of workforce members (Security) (Addressable)</td>
<td>Develop policies, procedures, and forms for documentation. Document measures.</td>
<td></td>
</tr>
<tr>
<td>Appropriate level of access (Security) (Addressable)</td>
<td>Must implement policies and procedures to ensure appropriate access to ePHI by establishing clear job descriptions and responsibilities. Develop policies and procedures. Document measures.</td>
<td></td>
</tr>
<tr>
<td>Appropriate criteria for access (Security) (Addressable)</td>
<td>Must implement policies and procedures to ensure appropriate access to ePHI by establishing criteria for hiring and assigning tasks. Develop policies and procedures. Document measures.</td>
<td></td>
</tr>
<tr>
<td>Establishment of workforce clearance (Security) (Addressable)</td>
<td>Must have process to determine whether a person should have access. Develop policies and procedures. Document measures.</td>
<td></td>
</tr>
<tr>
<td><strong>Breach Notification</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk assessment</td>
<td>Must have policies and procedures in place to determine whether a breach exists. Develop policies, procedures, and forms.</td>
<td></td>
</tr>
<tr>
<td>Type of Policy and Procedure</td>
<td>Comments</td>
<td>Completed</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------</td>
<td>-----------</td>
</tr>
<tr>
<td>Notification of Breach to individuals</td>
<td>Should have model forms for tracking, investigating, and providing notification of breach. Develop model forms.</td>
<td></td>
</tr>
<tr>
<td>Timeliness of Notification of Breach</td>
<td>Should have process to provide timely notification. Develop policies and procedures.</td>
<td></td>
</tr>
<tr>
<td>Notification of Breach methodology</td>
<td>Documents providing methods for notifying individuals will be compared to actual performance. Develop policies and procedures, including means to notify next of kin or personal representative and how to follow up if contact information is insufficient.</td>
<td></td>
</tr>
<tr>
<td>Notification Content</td>
<td>Notices must have specific content. Develop standard templates or forms.</td>
<td></td>
</tr>
</tbody>
</table>
Critical considerations when conducting a risk analysis of mobile devices.

*Who owns the device?* A different level of control exists if the device is owned by an individual employee or if it is actually a device owned by an organization. If a mobile device is owned by an organization, the organization can control the nature and content of that device.

*Are personal devices that are used at work registered?* If personal devices can be used to access, store, or transmit PHI, the question should be asked as to whether employees should be required to register those devices. Many organizations have centralized security management to make sure mobile devices accessing their internal networks or resources are compliant with their security policies. Centralized security management includes: (1) configuration requirements, such as installing remote disabling on all mobile devices; and (2) management practices, such as setting policy for individual users or a class of users on specific mobile devices.

*Is a virtual private network (VPN) used to exchange information so the information does not actually reside on the device? (Once the connection is broken, there is no information stored.)* With a VPN, the connection between a mobile device and a server is encrypted, so information sent or received is protected due to the encrypted tunnel established by the VPN, even on an unsecured network. VPNs can reduce the risk of using a public Wi-Fi access point (hotspot) or public wired Internet connection such as at a hotel or airport. Otherwise, information can be intercepted between the mobile device and the system connection.

*Is PHI from mobile devices saved onto servers?* If PHI from mobile devices is saved onto servers, then a data backup would exist for any information saved on the mobile device even if it is lost or stolen.

*Can mobile devices be remotely wiped or disabled if they are lost or compromised?* If a mobile device is lost or stolen, there are two potential paths to reduce the risk that PHI can be compromised: remote wiping and remote disabling. Remote wiping is a feature for lost or stolen mobile devices that remotely erases all the data on the mobile device. Some mobile devices have built-in remote wipe capability that the organization or authorized user can enable. Remote disabling enables you to lock or completely erase data stored on a mobile device if it is lost or stolen. If the mobile device is recovered, it may be unlocked.

*Is your workforce properly trained?* Policies and procedures are not meant to be put into a binder and then hidden on a high shelf. They are intended to be used on a daily basis, and the OCR will take steps to see if your organization is doing what it said it would be doing in your policies and procedures with regard to mobile devices.
Best Practices for use of Mobile Devices

The direction that a company takes in response to the risk analysis questions above will require the development and implementation of best practices surrounding the use of mobile devices. Some best practices to consider are:

- Enabling or installing security software and with a process in place to ensure that the software is kept up-to-date
- Researching apps before downloading to ensure the apps are do not create security gaps
- Implementing policies that emphasize maintaining physical control of devices
- Training employees to use caution when using Wi-Fi – particularly free Wi-Fi – due to increase security risk and risk of casual exposure of PHI through onlookers
- Deleting all stored ePHI before reusing or discarding mobile device
- Establishing a policy and process for employees to use password protection or some authentication key to disable access if mobile device is lost or stolen
- Avoid storing data locally on mobile device
- Require encryption for mobile devices
- Disable file-sharing on mobile devices
Five Steps to Developing Policies and Procedures for Use of Mobile Devices

1. Decide how PHI will be accessed, received, transmitted, or stored via a mobile device, and how mobile devices will be used as part of your organization's internal networks and other systems
   - For example, will ePHI be stored on a laptop? Will emails containing ePHI be accessible via a personal cell phone? How is that information stored on a network system?

2. Conduct a risk analysis
   - For example, will the mobile device be taken outside of the workplace? If so, what are the risks that the laptop will be lost or stolen?

3. Determine risk management strategy, including privacy and security safeguards
   - For example, will you require all employees who receive email containing PHI to password protect their cell phones?

4. Develop reasonable and appropriate policies and procedures for mobile devices
   - Your organization should have a mobile device management policy. That policy should address how to inventory those devices, what's on those devices, and what those devices are. That also means being aware, not only of the devices that you own, but the devices that your employees own, and on which device PHI may either be stored or pass through. This requires a decision as to whether to allow employees to utilize their own devices as part of handling PHI. Consider what restrictions to impose on mobile use and what security configurations and technical controls should be placed.

5. Conduct training
   - Train employees on how to physically secure the mobile devices so the chances of them being lost or stolen are reduced. Theft or loss is the most likely source of a breach.