NATIONAL
RURAL HEALTH
RESOURCE CENTER

Privacy and Security Overview and Resource List

Compliance with Law and Policy

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is the legal framework for the privacy and security of protected health information (PHI) or electronic protected health information (EPHI). When covered entities and other participants exchange EPHI, the actual exchange of information may be facilitated and even enhanced if all participants adopt and adhere to the same or consistent safeguard policies and procedures.

Covered entities must comply with applicable law and policies as well as provide patients required policies with their practice or hospital. If there are conflicts between sub-network organizations (SNO) policies and participant policies, the participant must follow the policy that is most protective of individual privacy. This deference to more protective policies echoes the HIPAA federal pre-emption requirements, which do not preempt more protective state privacy laws. Covered entities in a multi-jurisdictional environment must recognize more stringent privacy laws that will affect the exchange of EPHI across State lines. In addition, other Federal laws also may apply more stringent or different requirements to such exchanges depending on the circumstances.

PHI is the individually identifiable information created, received or maintained by (or on behalf) of a covered health care provider or a health plan or other HIPAA covered entity. Health information is linked to an individual from a set of 18 identifiers[1]. If these identifiers are removed, the information is de-identified and no longer PHI.

Whereas the HIPAA Privacy Rule deals with PHI, the HIPAA Security Rule deals with EPHI, which is essentially a subset of what the HIPAA Privacy Rule. The HIPAA Security Rule requires implementation of three types of safeguards: 1) administrative, 2) physical, and 3) technical and other organizational requirements (this will be discussed in more detail later in the guide).

The HIPAA Security Rule establishes national standards to protect individuals' EPHI that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. The Privacy Rule establishes a federal baseline of privacy protections and rights, which applies to covered entities consistently across state borders. The Privacy Rule, however, as required by HIPAA, does not preempt State laws that provide greater privacy protections and rights.

Participants must develop internal policies that will help implement the principles of sound data management practices and accountability as well as ensure that decisions affecting

[1] http://privacyruleandresearch.nih.gov/pr_08.asp

individuals' privacy interests are made thoughtfully, rather than case by case. Written documentation of such policies facilitates the training of personnel who will handle health information and enhances the accountability of both participants and members of their workforce.

Some of the major topic areas for policy development include (but are not limited to):

- Access
- Authorization
- Business Associates
- Confidentiality Agreement for various roles
- Data backup and Use
- Email Use
- Emergency Access
- Staff termination/Access revocation
- USB/Portable devices
- Release (s) of Information
- Consents
- Audits
- Notices to patients

Notice of Privacy Practices

Covered entities must provide patients with full information on how their PHI is used and disclosed. This is typically accomplished by giving patients a Notice of Privacy Practices that describes how an individual's information may be used or shared and specifies an individual's legal rights with respect to their protected health information held by the covered entity and the covered entity's legal duties.

HIPAA requires the Notice of Privacy Practices to include a description, with at least one example of the actual types of uses and disclosures that are permitted for treatment, payment and healthcare operations. Additionally, it is required that a description of other permitted purposes to use or disclose protected health information without individual authorization is included. HIPAA does not require the Privacy Notice to spell out what specific information may be disclosed and who may access the information.

Individual Participation and Control of Information Posted to Record Locater Service (RLS)

This recommended provision provides greater privacy protection over personal health information than the Privacy Rule by allowing individuals to elect whether or not to have information about them included in the RLS. This promotes the privacy principles of individual participation and control, purpose specification and minimization, use limitation, and collection limitation. Individuals are treated as participants in the process of health information collection and dissemination, rather than as spectators. By enhancing reasonable individual control over the collection and use of health information, this provision will promote consumer confidence that health information is being used and collected in accordance with individual preferences. The guidelines involve:

1. Choice Not to Have Information Included in the RLS: All individuals may choose not to have information about them included in or made available through the RLS.
2. Effect of Choice: An individual's choice not to have information about him or her included in or made available through the RLS shall be exercised through the Participant, as described in the institution's Notice, after which time the institution shall no longer include the individual in the RLS. Participants shall develop and

implement appropriate mechanisms to remove information about an individual from the RLS if the individual chooses to have such information excluded from the RLS.

3. Revocation: An individual who has chosen not to make information concerning him or her available through the RLS subsequently may be included in the RLS only if the individual revokes his or her decision or subsequently chooses to renew participation in the RLS.
4. Documentation: Each Participant shall document and maintain documentation of all patients' decisions not to have information about them included in the RLS.
5. Participant Choice: Participants will establish reasonable and appropriate processes to enable the exercise of a patient's choice not to have information about him or her included in the RLS. Each Participant retains the authority to decide whether and when to obtain patient consent prior to making information available through the RLS.
6. Provision of Coverage or Care: A Participant shall not withhold coverage or care from an individual on the basis of that individual's choice not to have information about him or her included in the RLS.

Uses and Disclosures of Health Information

This provision includes the principles of purpose specification and minimization, access controls, use limitation, collection limitation, accountability and oversight, and data integrity and quality. Access controls rely on authentication to verify user identify and authorizations to use specific resources/modules. Users must be authorized to access information through the HIE that is consistent with their job functions.

Hospitals and centers may conduct quarterly audits of authorized user accounts and compare the information accessed to the care that was provided by the authorized user. They may restrict the role-based access to the HIE based on the authorized user's current employment responsibilities. Workforce employees will have their access level noted in the HIE usage file and be reviewed regularly by their supervisor and/or the Privacy Officer.

An authorized user who accesses EPHI through the system will attest to the purpose of their access every time data is viewed. Authorized users may receive a unique user name that is connected to all authentication attempts. A unique identifier allows the tracking of specific user activity when that user is logged into an information system. Users can be held accountable for functions performed on information systems with EPHI when logged into these systems.

Users are trained to logoff the system when their workstation is unattended. Automatic logout is another effective way to prevent unauthorized users from gaining access to an unattended workstation.

Audit controls use digital certificates, encryption, and user authentication for each action. Additionally, in audit list queries hidden names or assigned numbers are used. Other data integrity security measures may include:

- Encryption: All EPHI and user authentication data is encrypted.
- User Authentication: The process will verify that an authorized user's identity is accurate. Users may have established roles and the appropriate access outlined through a User Agreement for Authorized Use. Each authorized user has a unique user name and password that may be changed every 90 calendar days.
- Message Integrity: Through the use of a Public Key Infrastructure (PKI), this message level protection prohibits unauthorized modification, often by the originator of the message generating a digital signature.

- Non-Repudiation: This non-changeable element that verifies the user that completed the action – allows for monitoring and audits. These controls may reduce prohibit any program, routine, subroutine, or data designed to disrupt the proper operation of a system or any part of hardware (including laptop computers) or software.

Information Subject to Special Protection

This recommended provision facilitates individualized privacy protections by requiring that participants are aware of special protections of information set forth under law (federal, state, and/or local) such as substance abuse, mental health, and/or HIV.

Participants' collection, use, and disclosure of PHI and EPHI will be limited to legitimate purposes and will defer to the law or policy most protective of an individual's privacy. Each participant is responsible for determining and identifying what information is subject to special protection under applicable law prior to disclosing any information through the HIE. Categories that may warrant a higher degree of security in an EHR system: diagnosis or condition, procedures or testing, consent and custody, and research.

Minimum Necessary

HIPAA requires that entities disclose only the amount of information reasonably necessary to achieve a particular purpose. Reasonable minimum necessary procedures can be implemented to limit how protected information is used, disclosed and requested in accordance with all federal and state laws. Additionally, an authorized user who accesses EPHI through the system will attest to the purpose of their access every time data is viewed. Users will have access to only the e PHI necessary to perform their specific work assignments and to prevent access for those that may have different information needs.

The minimum necessary standard, a key protection of the Privacy Rule, is derived from confidentiality codes and practices in common use today. It is based on sound current practice that PHI should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function. The minimum necessary standard requires covered entities to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of protected health information.

The Privacy Rule generally requires covered entities to take reasonable steps to limit the use or disclosure of, and requests for, protected health information to the minimum necessary to accomplish the intended purpose. The minimum necessary standard does NOT apply to the following:

- Disclosures to or requests by a health care provider for treatment purposes.
- Disclosures to the individual who is the subject of the information.
- Uses or disclosures made pursuant to an individual's authorization.
- Uses or disclosures required for compliance with the Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification Rules.
- Disclosures to the Department of Health and Human Services (HHS) when disclosure of information is required under the Privacy Rule for enforcement purposes.
- Uses or disclosures that are required by other law.

The implementation specifications for this provision require a covered entity to develop and implement policies and procedures appropriate for its own organization, reflecting the entity's business practices and workforce. While guidance cannot anticipate every question

or factual application of the minimum necessary standard to each specific industry context, where it would be generally helpful we will seek to provide additional clarification on this issue in the future. In addition, the Department will continue to monitor the workability of the minimum necessary standard and consider proposing revisions, where appropriate, to ensure that the Rule does not hinder timely access to quality health care.

Workforce, Agents and Contractors

By incorporating HIPAA's administrative requirements for workforce training, sanctions for privacy violations, and the reporting of complaints, this provision advances the privacy principles of use limitation, security safeguards and controls, accountability and oversight, data integrity and quality, and remedies.

Participants are responsible for developing and implementing a training program for its workforce members, agents, and contractors who will have access to the HIE to ensure compliance with the individual center's policies. Training will be held annually at a minimum and will cover:

- Confidentiality of PHI and EPHI under HIPAA
- Access to HIE for purposes of treatment of an individual or necessary health care operations.

An assigned Privacy/Security Officer may regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports and maintain/report discrepancies. Additionally, the Privacy/Security Officer may maintain a comprehensive listing of hardware and software used to store and transmit ePHI. Basic password safeguards may also be effective including: devising secure passwords, storing passwords, regularly changing passwords, avoidance of sharing passwords, and locking out users after multiple failed attempts.

The foundation of a complete security management process involves policies and procedures that are consistently verified. A hospital or center must have breach and security notification procedures in place that are in compliance with HIPAA and HITECH standards. Any unauthorized acquisition, access, use or disclosure of ePHI that compromises the security or privacy of PHI would be considered a HIPAA breach. As part of HIE, both federal and applicable state laws must be reflected in all privacy and security policies.

The hospital or center may identify and respond to suspected or known security incidents and mitigate the harmful effects of security incidents and appropriately document the incidents and outcomes. The Privacy/Security Officer may be responsible for developing and maintaining standards, providing implementation guidelines, and providing security training.

Amendment of Data

This provision integrates the right granted by the Privacy Rule that individuals can amend health information about them if it is incomplete or inaccurate. A covered entity that receives an amendment request will make reasonable efforts to provide the amendment. Denied requests must be in writing and made available to the patient requestor. The patient also has a right to submit a statement of disagreement for inclusion in his/her record.

This process promotes the privacy principles of data integrity and quality, openness and transparency, individual participation and control, and accountability and oversight. This applies to all organizations that have registered with and participating in the SNO. If an individual requests and the covered entity accepts, an amendment to the health information, they will make reasonable efforts to inform other participants that accessed or received such information through the SNO, within a reasonable time.

Requests for Restrictions

This provision requires participants who agree to requests for restrictions of individual's health information to comply with regard to the release of information in the SNO. Under the Privacy Rule, individuals have a right to request restrictions on the use and/or disclosure of health information about them. The Privacy Rule permits a covered health care provider to use or disclose protected health information for treatment purposes. Individuals have a right to request that the information is restricted but a covered entity is under no obligation to agree to requests for restrictions – the covered entity must have a procedure to evaluate all requests.

While in most cases, the treatment will be provided to the individual, the Rule does allow the information to be used or disclosed for the treatment of others. Therefore, the Rule does permit a doctor to disclose protected health information about a patient to another health care provider for the purpose of treating another patient (e.g., to assist the other health care provider with treating a family member of the doctor's patient). For example, an individual's doctor can provide information to the doctor of the individual's family member about the individual's adverse reactions to anesthetics prior to the family member undergoing surgery. These uses and disclosures are permitted without the individual's written authorization or other agreement with the exception of disclosures of psychotherapy notes, which requires the written authorization of the individual.

However, the Rule permits but does not require a covered health care provider to disclose the requested protected health information. The doctor with the protected health information may decline to share the information even if the Rule would allow it. The Rule may also impose other limitations on these disclosures.

Under 45 CFR § 164.522, individuals have the right to request additional restrictions on the use or disclosure of protected health information for treatment, payment, or health care operations purposes. If the health care provider has agreed to the requested restriction, then the doctor is bound by that agreement and (except in emergency treatment situations) would not be permitted to share the information. However, the health care provider maintaining the records does not have to agree to the requested restriction. For example, an individual who has obtained a genetic test may request that the health care provider not use or disclose the test results. If the health care provider agrees to the restriction, the information could not be shared with providers treating other family members who are seeking to identify their own genetic health risks.

Individuals do not have a right under the Rule to request that a covered entity restrict a disclosure of protected health information about them for workers' compensation purposes when that disclosure is required by law or authorized by, and necessary to comply with, a workers' compensation or similar law.

Mitigation

By incorporating HIPAA's requirement that entities have procedures involving harm mitigation resulting from an impermissible use or disclosure of health information, this model policy reflects the privacy principles of remedies, accountability and oversight, security safeguards and controls, openness and transparency, and data integrity and quality.

Under the Security Rule, a covered entity must mitigate, to the extent practicable, any harmful effects that are known to the covered entity and that result from a use or disclosure of PHI in violation of its own privacy policies and procedures or the Rule by the covered entity or its business associates. Mitigation is required for known harmful effects caused by the covered entity's own workforce misusing or disclosing electronic PHI or by such misuse or wrongful disclosure by a HIO that is a business associate of the covered entity. While appropriate steps to mitigate harm caused by an improper use or disclosure in an electronic environment will vary based on a totality of the circumstances, some mitigation steps to consider would be:

- Identifying the cause of the violation and amending privacy policies and technical procedures, as necessary, to assure it does not happen again;
- Contacting the network administrator, as well as other potentially affected entities, to try to retrieve or otherwise limit the further distribution of improperly disclosed information;
- Notifying the individual of the violation if the individual needs to take self-protective measures to ameliorate or avoid the harm, as in the case of potential identify theft.

Other Considerations

Healthcare organizations handle the most sensitive and personal data; patient demographics, patient insurance, patient credit and financial information. According to the 2008 HIMSS Analytics Report[2]: Security of Patient Data, in the period from 2006-2007, over 1.5 million names were exposed during data breaches that occurred in hospitals alone. Some breaches involve stolen or lost hardware, however data security can be compromised when a computer screen is left unattended.

Medical records have shifted from paper to electronic and therefore increasing the potential for individuals to access, use, and disclose sensitive personal health data. As a result, federal laws have expanded to address the privacy and security concerns of PHI and electronic health information.

The increased mobility of data leads to increased risk too. A Symantec/Ponemon[3] survey found that over 88% of companies surveyed experienced some level of data loss. The average cost of a breach was $7.2 million and the most common methods of 'taking data' include:

- Copying to CD/DVD
- Copying to USB Drives
- Sending to personal email accounts

Physical Safeguards from HIPAA

[2] http://www.mmc.com/views/Kroll_HIMSS_Study_April2008.pdf
[3] http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=ponemon
Symantec recommends the use of a data breach review calculator
https://databreachcalculator.com/GetStarted.aspx

Physical safeguards are in place to protect data from fire and other natural and environmental hazards and intrusion. Member hospitals within the National Rural Health Resource Center must maintain a secure environment that supports the use of electronic PHI and prevents disclosure[4].

Each hospital or center may have a plan for disaster recovery that includes a strategy and method for recovering lost or inaccessible PHI in a timely manner after a disaster. Their risk analyses including application and data criticality analysis may determine the order, interval of time, and the methods chosen for recovery. This may include additional security at entrances or escorts for authorized users to the facility for data restoration purposes. Procedures will also identify personnel that are allowed to re-enter the facility to perform data restoration.

The risk management plan may include a procedure to create and maintain data backups to ensure that information will not be lost in the event of a major system loss. Additionally the plan may determine what information requires back up, the appropriate backup mechanism (e.g., magnetic tapes, paper, or other medium), how to maintain the backups (e.g., offsite, in an air conditioned compartment or other conditions), and duration of maintenance (e.g., six months or following state/territory or federal guidelines for patient records).

Facility Access Controls

Securing physical access to electronic information systems and the facility or facilities in which they are housed, while also providing that all properly authorized persons have adequate access is a considerable effort. Hospitals or centers can evaluate the adequacy of controls on physical access to facilities and equipment as part of a regular security risk assessment. As part of its risk management plan, centers can document and have available for inspection, the facility access control and equipment handling logs. If the hospital or center does not control the building they occupy or shares space with other organizations, it nonetheless remains responsible for considering facility security. It can incorporate security measures into contracts with the party responsible for the building and document them in their own plan.

Unauthorized physical access to the facility may be limited via door locks, electronic access control systems, security officer (for larger facilities), and video monitoring. Additionally, facilities will have major doors re-keyed, door combinations changed, and/or key cards destroyed after the termination of employees or contractors with prior access to facilities that stored electronic PHI.

End Use/Security and Device/Media Controls

This concerns the use of a workstation, desktop or laptop. Each hospital or center can maintain a log governing the receipt and removal of hardware and electronic media that contains electronic PHI into and out of a facility, and the movement of these items within the facility. Inappropriate use of computer workstations can expose a facility to risks such as viruses, compromise of information systems, and breeches of confidentiality. Basic

[4] HIPAA Privacy and Security Rule, 45 Code of Federal Regulations (CFR) Parts 160 and 164. 45 C.F.R. § 164.310(a)(1-2), (d)(1)

security measures for workstation security include privacy screens, screen savers with password options, timed log-outs.

Property controls such as property control tags and the engraving of equipment may be completed on all media assets. Each hospital or center may maintain a log governing the receipt and removal of hardware and electronic media that contains electronic PHI into and out of a facility, and the movement of these items within the facility. When evaluating and implementing these standards, there must be consideration for all physical access to electronic PHI. This may extend outside of an actual office, and could include workforce members' homes, satellite offices, or other physical locations where they access electronic PHI.

Internal software license inventory records may be updated to reflect any transfer or deletion of software. Electronic media that contains e-PHI must be rendered unusable or inaccessible. Degaussing uses a magnetic field to erase the data. Destroying the media makes the data inaccessible. If circumstances warrant the destruction of the electronic media prior to disposal, destruction methods may include disintegrating, pulverizing, melting, incinerating, or shredding the media.

Certain steps are taken to remove the ePHI stored on the computers or other media before its disposal or reuse, or if the media itself is destroyed before its disposal.

The HIPAA Privacy and Security Rule requires that covered entities address the final disposition of ePHI and/or the hardware or electronic media on which it is stored, as well as to implement procedures for removal of ePHI from electronic media before the media are made available for reuse. Disposal of all technology hardware, software and paper records must be in accordance with federal, state, and local laws, including, but not limited to regulating waste and respecting copyright and licensed software. Sensitive information is protected and must follow all HIPPA specific policies and procedures.

Technical Safeguards from HIPAA

Technical safeguarding involves building defenses against unauthorized access to data over communication networks.

Access Control

Access controls rely on authentication to verify user identify. The access controls process will check that the user has been authorized to use that resource/module. Users must be authorized to access information through the HIE that is consistent with the job functions as determined.

Hospitals and centers may conduct quarterly audit authorized user accounts and compare the information accessed to the care that was provided by the authorized user. They may restrict the role-based access to the HIE based on the authorized user's current employment responsibilities. Workforce employees will have their access level noted in the HIE usage file and be reviewed regularly by their supervisor and/or the Privacy Officer. Changes in access levels will be made quickly and documented in the employee's file. The access is first authorized then later access requests are approved or disapproved based on the previously

defined authorizations. An authorized user who accesses ePHI through the system will attest to the purpose of their access every time data is viewed.

Audit Controls
This can involve the use of digital certificates, encryption, user authentication for each action, hidden name or assigned number in audit list queries and role-based access.

Integrity
The security measures may include: encryption, user authentication, message integrity, and support for non-repudiation. Definitions of the measures are as follows:

- Encryption: All ePHI and user authentication data is encrypted.
- User Authentication: The process will verify that an authorized user's identity is accurate. Users may have established roles and the appropriate access outlined through a User Agreement for Authorized Use. Each authorized user has a unique user name and password that may be changed every 90-calendar days.
- Message Integrity: Through the use of a Public Key Infrastructure (PKI), this message level protection prohibits unauthorized modification, often by the originator of the message generating a digital signature.
- Non-Repudiation: This non-changeable element that verifies the user that completed the action – allows for monitoring and audits. These controls may reduce prohibit any program, routine, subroutine, or data designed to disrupt the proper operation of a system or any part of hardware (including laptop computers) or software.

Person or entity authentication
Authorized users may receive a unique user name that is connected to all authentication attempts. A unique identifier allows the tracking of specific user activity when that user is logged into an information system. Users can be held accountable for functions performed on information systems with e-PHI when logged into these systems.

User identification is a way to identify a specific user of an information system, typically by name/number. At a minimum, the employee name or some variation of the name can be used. However, a highly recommended system is a set of random numbers and characters. This may be harder for an authorized user to remember but more likely to keep an unauthorized user from gaining inappropriate access.

Transmission security
Users are trained to logoff the system when their workstation is unattended. Automatic logout is an effective way to prevent unauthorized users from gaining access to an unattended workstation.

Legal/Compliance Officer
The healthcare Legal/Compliance Officer establishes and implements an effective compliance program to prevent illegal, unethical, or improper conduct. The Legal/Compliance Officer acts as staff to the CEO and Governing Board by monitoring and reporting results of the compliance and ethics efforts of the company and in providing guidance for the Board and senior management team on matters relating to reporting and compliance. The Legal/Compliance Officer, together with the Corporate Compliance Committee, is authorized to implement all necessary actions to ensure achievement of the objectives of an effective compliance program.

Administrative Safeguards from HIPAA

Administrative safeguards involve the operations and oversight of physical and technical safeguards, including systematic, auditable security policies and processes.

Security Management Process/Assigned Security Responsibility
The foundation of a complete security management process involves policies and procedures that are consistently verified. A hospital or center must have breach and security notification procedures in place that are in compliance with HIPAA and HITECH standards. Any unauthorized acquisition, access, use or disclosure of ePHI that compromises the security or privacy of PHI would be considered a HIPAA breach. As part of HIE, both federal and applicable state laws must be reflected in all privacy and security policies.

Workforce Security
An assigned Privacy/Security Officer may regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports and maintain/report discrepancies. Additionally, the Privacy/Security Officer may maintain a comprehensive listing of hardware and software used to store and transmit e PHI. Basic password safeguards may also be effective including: devising secure passwords, storing passwords, regularly changing passwords, avoidance of sharing passwords, and locking out users after multiple failed attempts.

Information Access Management
Users will have access to only the e PHI necessary to perform their specific work assignments and to prevent access for those that may have different information needs. Additionally, when a user ceases to require access to e PHI, access must be immediately restricted or removed.

Security Training and Incident Procedures
The hospital or center may identify and respond to suspected or known security incidents and mitigate the harmful effects of security incidents and appropriately document the incidents and outcomes. The Privacy/Security Officer may be responsible for developing and maintaining standards, providing implementation guidelines, and providing security training.

Contingency Plan
The hospital or center may have a contingency plan including a procedure to create and maintain data backups. The "data backup" portion of a contingency plan should ensure that information will not be lost in the event of a major system loss. A hospital or center may determine what information requires backup, the appropriate backup mechanism (e.g., magnetic tapes, paper, or other medium), how to maintain the backups (e.g., offsite, in an air conditioned compartment or other conditions), and duration of maintenance (e.g., six months or following state/territory or federal guidelines for patient records).

Privacy and Security within a HIE

Many providers elect to build their own HIE, which is both funded and operated by an individual provider organization or is a collaborative of providers. Most privately built HIEs are owned and operated by hospitals or hospital systems due to the capital requirements and necessary policy development. Benefits of building an
HIE include tailoring use-cases directly to your provider's needs, controlling the storage and usage of all data within the network, and ability to set privacy and security controls.

Protecting patients' privacy and securing their health information is a core requirement for the Medicare and Medicaid Electronic Health Record (EHRs) Programs. The Medicare and

Medicaid EHR Incentive Programs are referred to as the "Meaningful Use Programs". Further, effective privacy and security measures protect your clinical practice from civil and criminal penalties.

A recent article in Healthcare IT News[5] suggested several common gaps in healthcare data security and privacy. Despite the HIPAA rules for security and privacy safeguards were extended by the HITECH Act, many gaps still remain. The following rules may help address privacy and security gaps:

Avoid access to data from unauthorized individuals
Users often leave computers logged-in while they are away from their desks. Areas of limited and restricted access must be monitored. A walk-through, during and after business hours, can help providers identify whether unauthorized people can physically gain access to protected data.

Monitor controls on key systems and check for inadequate logging
Every time system users access computerized records, they leave an electronic footprint, or log, on the information systems. Most healthcare organizations rely on access controls to help ensure compliance with the HIPAA Security Rule. However, security gaps occur when providers use antiquated systems that don't allow logging, update to new systems without enabling logging or simply don't adequately monitor logged activities.

Protect access control
Providers should confirm that passwords are required to access all of their systems, databases and applications that house PHI. All required passwords should meet complexity requirements, such as including a combination of numbers, symbols, uppercase and lowercase letters, and be reset on a regular basis. Accounts should be locked after a series of failed log-in attempts, and a log should be made of all failed log-in attempts so accounts that are being targeted for compromise can be more easily identified.

Create strong vendor management functions
Most providers do not maintain a comprehensive list of Business Associate (BA) agreements that include the type of data being shared with the BAs. The HIPAA Privacy Rule requires that the "minimum necessary" standard be applied to any data shared with vendors. Vendor management has a lifecycle of its own and should be viewed and managed as such in order to appropriately protect PHI.

Develop business continuity management and incident response plans
Many providers have a disaster recovery plan that provides guidance on how patient care should continue in the event that IT systems are unavailable. This approach leaves a gap with regards to the prioritization and recovery efforts of systems in the event of an incident. An information security-specific disaster recovery plan should be part of this plan, while a computer security incident response plan should also be developed in case of a breach.

Make Patients Aware of Opt-in or Opt-out Policies
Providers should consider ensuring that each patient is aware of the policies regarding participation in an HIE. Many HIEs offer an Opt-out system, where information on every patient is added to the network. In this scenario, each patient is assumed to consent to including their information in the data exchange and only patient who directly express a lack of consent have their information removed. Another common privacy policy is the Opt-out

[5] https://www.healthcareitnews.com/news/top-5-most-common-gaps-healthcare-data-security-and-privacy

system. In this scenario, only information on patients who have directly given their consent can have data within the exchange network.

Opt-in systems inherently require the patient to understand how their data is being used. Conversely, patients may be unaware of the changes in data exchange within an Opt-out system. It can be important to clearly explain to patients how their information will be used, thus ensuring patients trust their records are being kept private, even within an Opt-out exchange.

Preparing for an Internal Audit

An internal audit can be performed in phases, including data gathering, analysis, and reporting. Each phase may enable reviewers to properly formulate the recommendations needed (both tactical and strategic). The first phase involves site visits, interviews, and observations.

Each hospital or center may require a review of Security Policies and Procedures compared against the applicable HIPAA Security Standards and Implementation Specifications highlighting points of compliance, partial compliance, and non-compliance (gaps). Through interviews and observations there may be a review of the security established over technical infrastructure including network and server infrastructure, applications, workstations and mobile computing devices, database management systems and other tools, data center operations and IT services, as well as physical security over computing devices.

Vulnerability and penetration tests of systems may be recommended to identify weaknesses (also referred to as security "holes") in security protocols such as, by way of example only, out-of-date security updates (patches, packs, hot-fixes), open but unused ports, null and default administrative passwords in place, presence of EPHI and other sensitive data on insecure share drives, obsolete operating systems, out-of-date anti-virus and other malware protections, and similar issues. There may also be significant review including:

- Enterprise Organization Chart
- IT Organization Chart
- Security Policies and Procedures
- Long-range IT Plan (if available)
- Network Diagram (LAN and WAN)
- Network Device Inventory (routers, switches, access points, etc.)
- Server Inventory
- Applications Inventory
- DBMS Inventory
- Application Integration Architecture or Chart
- Interface Engine Inventory (if applicable)
- Report Writer/Query Tools Inventory
- Anti-virus and similar security software inventory
- Security and Network Products Inventory (e.g., IDS, VPN, Network Monitoring, RADIUS, RAS, etc.)
- E-mail Products Inventory
    - Firewall inventory and rules
    - Review and cross-walk Security Policies and Procedures
    - User interviews regarding policy compliance—up to 20, to be combined with the Privacy interviews
    - IT Personnel interviews:
        - IT Director

    - Security Officer/Official/Manager/Administrator
    - Network Administrators/Engineers
    - Server Administrators
    - Application Analysts/Administrators, including DBA's (or equivalent)
    - IT Operations Manager (or equivalent)
    - Help Desk Manager/Administrator
    - Web Serves Administrator
- Other interviews:
    - Education Manager (or Human Resources if responsible for training)
- View the facility, data center, and IT department---physical security observations
- Plan and perform the vulnerability and penetration testing
- Plan and perform the Social Engineering testing
- Analyze data collected (interviews and observations) and prepare findings documentation
- Perform any follow-up interviews or analysis as may be needed meaningful use of health information technology.

Centers for Medicare and Medicaid (CMS) assessed compliance with the Administrative, Physical and Technical Safeguards, Remote Access and Organizational, Policies and Procedures and Documentation Requirements areas of the Security Rule. CMS's particular focus for these reviews included, but was not limited to, the following areas:

- Risk analysis and management;
- Security training;
- Physical security of facilities and mobile devices,
- Off-site access and use of EPHI from remote locations;
- Storage of EPHI on portable devices and media;
- Disposal of equipment containing EPHI;
- Business associate agreements and contracts;
- Data encryption;
- Virus protection;
- Technical safeguards in place to protect EPHI; and
- Monitoring of access to EPHI

The objective of a review is to assess compliance with the HIPAA Security Standard, including the reasonable identification of risks and vulnerabilities—technical, physical, administrative—to the security of patient information predominately in electronic form.

Additionally, when a user ceases to require access to EPHI, access must be immediately restricted or removed. Access controls rely on authentication to verify user identify. Users must be authorized to access information through the HIE that is consistent with the job functions as determined.

Hospitals and centers may conduct quarterly audit authorized user accounts and compare the information accessed to the care that was provided by the authorized user. They may restrict the role-based access to the HIE based on the authorized user's current employment responsibilities. Workforce employees will have their access level noted in the HIE usage file and be reviewed regularly by their supervisor and/or the Privacy Officer. Changes in access levels will be made quickly and documented in the employee's file. The access is first authorized then later access requests are approved or disapproved based on the previously defined authorizations. User identification is a way to identify a specific user of an information system, typically by name/number. At a minimum, the employee name or some variation of the name can be used. However, a highly recommended system is a set

of random numbers and characters. This may be harder for an authorized user to remember but more likely to keep an unauthorized user from gaining inappropriate access.

Authorized users may receive a unique user name that is connected to all authentication attempts. A unique identifier allows the tracking of specific user activity when that user is logged into an information system. Users can be held accountable for functions performed on information systems with e-PHI when logged into these systems.

Privacy and Security Resource Listing

This is a listing of HIPAA resources for staying current on state legislative changes:
http://aspe.hhs.gov/admnsimp/final/PvcPre02.htm
http://www.hhs.gov/ocr/privacy/index.html
http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html
http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html
http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html
http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/individualchoice.pdf
http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf
http://www.cms.gov/EHRIncentivePrograms/Downloads/EP-MU-TOC.pdf