The Office of the National Coordinator for Health Information Technology

Guide to Privacy and Security of Health Information

Chapter 4:

Integrating Privacy and Security into Your Practice

Version 1.1 022312

Putting the I in HealthIT
www.HealthIT.gov

Chapter 4:

Integrating Privacy and Security into Your Practice

Understanding Patients' Individual Rights and Provider Responsibilities

Ensuring privacy and security of electronic health information is a key component to building the trust required to realize the potential benefits of electronic health information exchange. If individuals and other participants in a network lack trust in electronic exchange of information due to perceived or actual risks to individually identifiable health information or the accuracy and completeness of such information, it may affect their willingness to disclose necessary health information and could have life-threatening consequences.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules protect the privacy and security of individually identifiable health information. Whether the information is on a computer, paper, or other media, you have responsibilities for safeguarding health information. The HIPAA Privacy Rule covers protected health information (PHI) in any medium, while the HIPAA Security Rule covers electronic protected health information (e-PHI). HIPAA Rules have detailed requirements regarding both privacy and security.

Your practice, not your electronic health record (EHR) vendor, is responsible for taking the steps needed to comply with HIPAA privacy, security standards, and the Centers for Medicare & Medicaid Services' (CMS') Meaningful Use requirements.

Read up on laws governing the privacy and security of health information. You must comply with all applicable federal, state, and local laws.

The HIPAA Privacy Rule

The HIPAA Privacy Rule[41] establishes a set of national standards for the use and disclosure of individually identifiable health information – often referred to as protected health information – by covered entities, as well as standards for providing individuals with privacy rights and helping individuals understand and control how their health information is used. HIPAA Privacy Rule requirements:

- Apply to most health care providers, including those who do not have EHRs or do not participate in a CMS EHR incentive program;
- Set a federal floor for protecting individually identifiable health information across all mediums (electronic, paper, and oral);
- Limits how covered entities may use and disclose individually identifiable health information they receive or create;
- Gives individuals rights with respect to their protected health information, including a right to examine and obtain a copy of information in their medical records, and the right to ask covered entities to amend their medical record if information is inaccurate or incompleted;
- Imposes administrative requirements for covered entities, such as training of employees with regard to the Privacy Rule; and
- Establishes civil penalties.

41 http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html

Violations of the Privacy Rule may be enforced through imposition of civil and criminal penalties. Learn more about **HIPAA enforcement**[42].

Several central tenets of the Privacy Rule are:

- In general, you may use or disclose protected health information for treatment, payment, and health care operations without obtaining a patient's written permission. For other purposes, such as marketing, you may need to obtain an individual's authorization to use or disclose the patient's protected health information.
- Your agreements with business associates must explicitly require them to comply with HIPAA, including breach notification requirements.
- Generally, you and your business associates must limit your access to, use of, and disclosure of protected health information to the minimum necessary to carry out an action. This is called the "minimum necessary rule." There are several exceptions to this rule. For example, generally, you do not have to limit the disclosure of protected health information to the minimum amount necessary when you are disclosing the information for treatment of the individual.

Related Topics

- Complying with Privacy & Security Requirements

Resources

- HIPAA Requirements in detail (OCR)
- The Privacy Rule, in detail (OCR)
- The Security Rule, in detail (OCR)
- Customized, on-the-ground assistance to providers
- Privacy and Security Resources

Patients' Rights and Your Responsibilities

Under HIPAA, patients have legal, individual rights to access their health information and learn about disclosures of their health information. As their health care provider, you are responsible for respecting these rights.

The U.S. Department of Health and Human Services Office for Civil Rights (OCR) explains these rights and other requirements in its **Summary of the HIPAA Privacy Rule**[43].

As a covered entity, you have responsibilities to patients under the HIPAA Privacy Rule, including:

- **Notice of privacy practices:** Under the HIPAA Privacy Rule, covered entities must provide patients with full information on how their protected health information is used and disclosed. This is accomplished by giving patients a Notice of Privacy Practices that describes how an individual's information may be used or shared, specifies an individual's legal rights with respect to their protected health information held by the covered entity (many of which are described below), and the covered entity's legal duties.

42 http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html
43 http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html

- **Patient access to their information:** Patients have the right to inspect, review, and receive a copy of health information about themselves held by covered entities or business associates in a designated record set, which includes a health care provider's medical and billing records. Generally, these health plans and providers have to comply with requests for access within 30 days.
- **Amending patient information:** Patients have the right to request that covered entities amend their protected health information in a designated record set when that information is inaccurate or incomplete. If a covered entity accepts an amendment request, it must make reasonable efforts to provide the amendment to persons that the individual has identified as needing it, and to persons that the covered entity knows might rely on the information. If the request is denied, covered entities must provide the individual with a written denial and allow the individual to submit a statement of disagreement for inclusion in the record.
- **Accounting of disclosures:** Individuals have a right to receive an accounting of disclosures, which is a listing of when a HIPAA covered entity has shared the individual's PHI with a person or organization outside of the entity. Accounting is only required for certain disclosure purposes. A covered entity must provide an accounting of disclosures made during the accounting period, which is six years immediately preceding the accounting request, but a covered entity is not obligated to account for any disclosure made before its Privacy Rule compliance date.
- **Rights to restrict information:** Individuals have the right to request that a covered entity restrict use or disclosure of protected health information for treatment, payment or health care operations, disclosure to persons involved in the individual's health care or payment for health care, or disclosure to notify family members or others about the individual's general condition, location, or death. A covered entity is under no obligation to agree to requests for restrictions; however, a covered entity must have a procedure to evaluate all requests. A covered entity that does agree must comply with the agreed restrictions, except for purposes of treating the individual in a medical emergency.

Designated Record Set

A designated record set is basically a group of records which a covered entity uses to make decisions about individuals, and includes a health care provider's medical records and billing records, and a health plan's enrollment, payment, claims adjudication, and case or medical management record systems.

For more information about what a designated record set, please see **OCR's website**[44].

44 http://www.hhs.gov/ocr/privacy/hipaa/faq/right_to_access_medical_records/311.html

HIPAA Limits on Using & Disclosing Patient Information

What types of information does HIPAA protect?

The Privacy Rule applies to all **PHI**[45] , which includes, when held or transmitted by a covered entity, information that:

- Relates to the individual's past, present, or future physical or mental health or condition; to the provision of health care to an individual; or to past, present, or future payment for the provision of health care to the individual; and
- Identifies the individual, or for which there is a reasonable basis to believe it can be used to identify the individual.

Protected health information can be in any form—electronic, paper, or oral—and includes financial and demographic information collected from patients.

Is there any information that is not restricted by HIPAA?

HIPAA Rules do not govern the use or disclosure of health information that does not identify an individual (known as "de-identified" PHI). Once PHI is de-identified in accordance with the HIPAA Privacy Rule, it is no longer PHI and, thus, may be used and disclosed by the covered entity or health information organization for any purpose (subject to any other applicable laws). You can share de-identified PHI, but just removing name, address, and social security number may NOT make information **"de-identified**[46]**"**. The Privacy Rule designates two processes through which a covered entity can determine that protected health information is de-identified.

Also, the HIPAA Rules do not apply to a covered entity's own employment records, or to education-related and certain other records covered by the **Family Educational Rights and Privacy Act (FERPA)**[47].

What about patient information pertaining to behavioral health or substance abuse?

The HIPAA Privacy Rule protects individually identifiable behavioral health or substance abuse information that a covered entity collects or maintains in a medical record in the same way that it protects other PHI.

HIPAA is not the only federal law that impacts the disclosure of health information. In some instances, a more protective law may require an individual's permission to disclose health information where HIPAA would permit the information to be disclosed without the individual's authorization. In addition, HIPAA does not override State law provisions that are at least as protective as HIPAA.

Do I need to inform my patients about how I use or disclose their health information?

Under the HIPAA Privacy Rule, covered entities must provide patients with a **Notice of Privacy Practices**[48] that specifies an individual's legal rights and the covered entity's legal duties with respect to the use and disclosure of PHI.

In addition to providing this notice to patients at the initial visit, a covered provider must make its notice available to any patient upon request.

45 http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html
46 http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/deidentificationworkshop2010.html
47 http://www2.ed.gov/policy/gen/guid/fpco/doc/ferpa-hipaa-guidance.pdf
48 http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/notice.html

Your practice has likely been using a Notice of Privacy Practices for several years now. If you need a template of an acceptable privacy practice, your REC or state or county medical association may be able to suggest some templates that comply with HIPAA requirements. Note that state and private sector requirements may necessitate adding other information to your notice. Plan to reassess your notice once OCR issues the final rule for the Health Information Technology for Economic and Clinical Health Act (HITECH) changes to HIPAA.

Please refer to OCR's website to **learn more about the notice**[49].

How to Keep Your Patients' Health Information Secure

A new EHR alters the mix of security needed to keep patient health information confidential. A new EHR also brings new responsibilities for safeguarding your patients' health information in an electronic form.

To uphold patient trust as your practice adopts an EHR, and to comply with HIPAA and meaningful use requirements, covered providers must conduct a security risk analysis. The risk analysis process will lead you to systematically examine many aspects of your medical practice:

- Your EHR software and hardware
- Adequacy of your practice protocols
- Physical setting and environment
- Staff education and training
- EHR access controls
- Contracts with your business associates
- Patient relations and communications

If you do not generally use e-PHI, you will likely need to make changes in the above areas to comply with HIPAA and Meaningful Use requirements. Fortunately, **properly configured, certified EHRs**[50] can provide more protection to patient health information than that provided by paper:

- Unique passwords and user names help prevent unauthorized access to the system.
- User and role based access controls prevent inappropriate or unauthorized access to both patient information and system controls.
- Backup and recovery is essential to ensuring availability of patient information to providing consistency in care.
- Encryption protects patient health information in transmission and on mobile devices, and is often a limit on liability for breach purposes under HIPAA.
- Appropriate and properly installed wireless capability provides firewalls and encryption functionality to keep your practice network secure.

49 http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/noticepp.html
50 http://healthit.hhs.gov/CHPL

The HIPAA Security Rule

The HIPAA Security Rule[51] establishes national standards to protect individuals' electronic protected health information 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 HIPAA Security Rule requires providers to implement security measures, which help protect patients' privacy by creating the conditions for patient health information to be available, but not be improperly used or disclosed. These requirements apply only to e-PHI.

All health care providers considered "Covered Entities" under HIPAA (most are) are responsible for complying with the two related rules of HIPAA: **Privacy**[52] and **Security**[53]. The HIPAA Security Rule sets out specific protections that all covered providers must follow to protect health information. These practices include administrative, technical, and physical safeguards. These safeguards, when applied well, can help practices avoid some of the common security gaps that lead to cyber-attack or data loss. They can protect the people, information, technology, and facilities that health care providers depend on to carry out their primary mission: helping their patients.

The HIPAA Security Rule requires three kinds of safeguards: administrative, physical, and technical.

51 http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html
52 http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html
53 http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html

Administrative safeguards

These safeguards establish standards and specifications for your health information security program that involve the following:

- Security management processes to identify and analyze risks to e-PHI and implementing security measures to reduce risks
- Staff training to ensure knowledge of and compliance with your policies and procedures
- Information access management to limit access to electronic health records to protect health information, including the information in EHRs
- Contingency plan to respond to emergencies or restore lost data

Physical safeguards

These safeguards control physical access to your office and computer systems. Examples of required physical safeguards include:

- Facility access controls, such as locks and alarms, to ensure only authorized personnel have access into facilities that house systems and data
- Workstation security measures, such as cable locks and computer monitor privacy filters, to guard against theft and restrict access to authorized users
- Workstation use policies to ensure proper access to and use of workstations

Technical safeguards

These safeguards include hardware, software, and other technology that limits access to e-PHI. Examples of required technical safeguards include:

- Access controls to restrict access to PHI to authorized personnel only
- Audit controls to monitor activity on systems containing e-PHI, such as an electronic health record system
- Integrity controls to prevent improper e-PHI alteration or destruction
- Transmission security measures to protect e-PHI when transmitted over an electronic network

Please visit the OCR for a full overview of security standards and required protections for e-PHI under the HIPAA Security Rule.

Working with Your EHR and Health IT Vendors

When working with your EHR and Health IT vendors, you may want to ask some of the following questions to help you ascertain some of the issues you need to address in your particular practice:

- Are the security features listed below in my certified EHR and my practice environment addressed in your implementation process? Will you train my staff on these features so they can update and configure as necessary?
  - Encryption
  - Auditing function
  - Firewalls and encryption on computer, software, and router
  - Backup and recovery
  - Unique IDs and passwords, biometric if available
  - Role based or user based access controls
  - Anti-virus and anti-spyware
- How does my backup and recovery system work, where is the documentation and how do I test this recovery system?
- How much of your EHR training covers privacy and security functions?
- Communications regarding updates, for example how will you know when valid EHR vendor staff are contacting your practice so that staff do not fall victim to social hacking?

Your EHR Software and Hardware

Most EHRs and the related equipment have these security features built into or provided as part of a service, although they are not always configured or enabled properly. As the guardian of patient health information, it is up to you to learn these basic features and along with your staff, ensure they are functioning and are updated when necessary. Remember, security risk analysis and mitigation is an ongoing responsibility for your practice. This should be part of your practice's ongoing activities and a full security risk analysis should be conducted at least once a year.

Cybersecurity

To exchange patient information, submit claims electronically, generate electronic records for patients' requests, or e-prescribe, an Internet connection is a necessity.

Strong cybersecurity practices are important in order to protect patient information, organizational assets, operations, personnel, and for compliance with the HIPAA Security Rule. Basic cybersecurity practices are needed to protect the confidentiality, integrity, and availability of electronic health record systems, regardless of how they are delivered—whether installed in a physician's office or accessed over the Internet.

Definition of Cybersecurity

Cybersecurity: The protection of information and systems that connect to the Internet. It is in fact protecting your personal information or any form of digital asset stored in your computer or in any digital memory device. It includes detection and response to a variety of cyber (online) attacks.

The U.S. Department of Health and Human Services Office of the National Coordinator for Health Information Technology's (ONC's) **Cybersecurity Checklist**[54] [PDF - 507 KB] shows you 10 simple best practices that should be taken to reduce the most important threats to the safety of EHRs.

For a full overview of **security standards and required protections for e-PHI under the HIPAA Security Rule**[55], visit OCR's website.

What to Do in Case of a Breach of Unsecured PHI?

Definition of e-PHI

Electronic Protected Health Information (e-PHI): The HIPAA Security Rule protects a subset of information covered by the HIPAA Privacy Rule. This subset of information is referred to as e-PHI. e-PHI is all PHI a covered entity creates, receives, maintains, or transmits in electronic form. The Security Rule does not apply to PHI transmitted orally or in writing.

The HIPAA Privacy Rule protects the privacy of individually identifiable health information, called protected health information (PHI). PHI includes information:

- That relates to the individual's past, present, or future physical or mental health or condition; to the provision of health care to an individual; or to past, present, or future payment for the provision of health care to the individual; and
- That identifies the individual, or for which there is a reasonable basis to believe it can be used to identify the individual.

A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.

The Breach Notification Rule

The Breach Notification Rule[56] requires HIPAA covered entities to promptly notify individuals and the Secretary of U.S. Department of Health and Human Services (HHS) of the loss, theft, or certain other impermissible uses or disclosures of unsecured protected health information. Health care providers must also promptly notify the Secretary of HHS if there is any breach of unsecured protected health information and if the breach affects 500 or more individuals, and notify the media if the breach affects more than 500 patients of a state or jurisdiction.

54 http://healthit.hhs.gov/pdf/cybersecurity/Basic-Security-for-the-Small-Healthcare-Practice-Checklists.pdf
55 http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html
56 The Breach Notification Rule is an interim final rule and subject to future final rulemaking.

- Significant breaches are investigated by OCR and fines may be imposed for failure to comply with the HIPAA Rules. **Breaches that affect 500 or more patients are publicly reported on the OCR website**[57].
- Similar breach notification provisions implemented and enforced by the **Federal Trade Commission**[58], apply to vendors of personal health records and their third party service providers.

Your Practice and the HIPAA Rules

Who Must Comply with HIPAA Rules?

"Covered entities[59]**"** must comply with the HIPAA Privacy and Security Rules:

- Health care providers, including doctors, clinics, hospitals, nursing homes, and pharmacies that electronically transmit any health information in connection with a transaction for which HHS has adopted a standard;
- Health plans; and
- Health care clearinghouses.

If you are a covered entity and you have a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity, the person or entity is considered a **"business associate**[60]**."**

As a covered entity, it is your **responsibility to obtain a written contract or agreement that the business associate will appropriately safeguard the PHI**[61] created or received on your behalf.

Where can I get help or more information?

Sixty-two Regional Extension Centers across the nation are prepared to offer customized, on-the-ground assistance to providers who are implementing HIPAA privacy and security protections.

57 http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html
58 http://www2.ftc.gov/opa/2009/08/hbn.shtm
59 http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html
60 http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html
61 http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html

Failure to Comply with HIPAA

Failure to comply with HIPAA can result in civil and criminal penalties.

Civil Penalties

OCR is responsible for administering and enforcing the HIPAA Privacy and Security Rules and conducts complaint investigations, compliance reviews, and audits. Fines may be imposed for failure to comply with the HIPAA Rules.

The civil penalties, especially for intentional disclosure of PHI are substantial, which makes compliance with the HIPAA Privacy and Security Rules essential.

State attorneys general may also enforce provisions of the HIPAA Rules.

Learn more about **OCR's HIPAA enforcement**[62], the **HIPAA Privacy & Security Audit Program**[63], or the **HIPAA Enforcement Rule**[64].

Criminal Penalties

The U.S. Department of Justice enforces criminal penalties for HIPAA violations.

Public Reporting of Breach Incidents

Breaches of unsecured PHI that affect 500 or more individuals are publicly reported on the OCR website[65].

Find out more about the **Breach Notification Rule and reporting requirements**[66].

Oversight

The Office for Civil Rights, within the U.S. Department of Health and Human Services (HHS) administers and enforces the HIPAA Privacy, Security, and Breach Notification Rules. State attorneys general may also enforce provisions of the HIPAA Rules. The Centers for Medicare and Medicaid Services within HHS oversees the EHR incentive programs. The Office of the National Coordinator for Health Information Technology provides support for the adoption and promotion of EHR and health information exchange (HIE) to improve health care in the United States.

Breach notification rule and reporting

62 http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html
63 http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html
64 http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/index.html
65 http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html
66 http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/

Compliance with Other Laws and Requirements

Besides HIPAA, HITECH, and Meaningful Use privacy and security-related requirements, your medical practice may also need to comply with additional privacy and security laws and requirements. To learn more about these other requirements, view the table below.

The table below provides a snapshot of these domains. Your state board of medicine and your state associations may also have guidance. Privacy and security requirements will continue to evolve. Stay abreast of them and integrate them into your medical practice.

Laws/ Requirements	Key Points
Sensitive Health Information	• Some laws and frameworks recognize that particular health conditions may put individuals at a higher risk for discrimination or harm based on that condition. Federal and some state laws require special treatment and handling of information relating to alcohol and drug abuse, genetics, domestic violence, mental health, and HIV/AIDs. • Federal laws: - 42 CFR Pt. 2: Confidentiality of Alcohol and Drug Abuse[65] - Family Education Rights and Privacy Act (FERPA)[66] - Genetic Information Nondiscrimination Act (GINA)[67] - Title X of Public Health Service Act - Confidentiality[68]
Minors' Health Information	• State and federal laws generally authorize parent or guardian access to minors' health information. • Depending on age and health condition (e.g., reproductive health, child abuse, mental health), and applicable state law, minors also have privacy protections related to their ability to consent for certain services under federal or state law. • Federal laws: - Family Education Rights and Privacy Act - Genetic Information Nondiscrimination Act - Title X of Public Health Service Act
Private-Sector Requirements	• A contracting health plan or payer may require confidentiality or safeguards.

67 http://www.samhsa.gov/healthPrivacy
68 http://www.samhsa.gov/healthPrivacy/
69 http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=ecbc0d928c8f11dbab0c20532d0101c9&rgn=div8&view=text&node=29:4.1.4.1.21.0.26.9&idno=29%20and%20http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=ecbc0d928c8f11dbab0c20532d0101c9&rgn=div8&view=text&
70 ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=ce18bb9053f3b026e8983fd8ac27170c&rgn=div8&view=text&node=42:1.0.1.4.43.1.19.11&idno=42

Essential HIPAA Terms to Know

Understanding your HIPAA responsibilities requires being familiar with the following terms:

- **Covered entities** include health plans, health care clearinghouses, and most health care providers. Most providers are covered entities because they transmit electronic health information in connection with a standard transaction adopted pursuant to HIPAA administrative simplification rules (e.g., billing electronically). Transmission also includes paper faxes and electronic submissions through an EHR or computer portal. Therefore, most provider practices will be covered entities under HIPAA.
- **Business associates** are individuals and organizations that perform services for or on behalf of your practice that entail routine access to protected health information. Examples: claims processing or administration. OCR provides more information about conduits of PHI.
- **Individually identifiable health information** ("IIHI"): Under HIPAA, IIHI is a subset of health information, and
  - (a) Is created or received by a health care provider, health plan, employer, or health care clearinghouse;
  - (b) Relates to past, present, or future health or condition of an individual, provision or care, or payment; and
  - (c) Identifies the individual or there is a reasonable basis to believe that the information could be used to identify the individual.
- **Protected health information (PHI)** refers to individually identifiable health information, that is:
  - (a) Transmitted by electronic media;
  - (b) Maintained in electronic media; or
  - (c) Transmitted or maintained in any other form or medium.

Not all IIHI is PHI. IIHI in the hands of a non-HIPAA covered entity is not PHI. IIHI in educational or employment records is not PHI, regardless if it is held by a covered entity.

HIPAA does not provide protections for all health information. HIPAA applies only to PHI.

- **De-Identified Health Information** is health information that does not identify an individual, and for which there is no reasonable basis to believe that it can be used to identify an individual. Once PHI is de-identified in accordance with the HIPAA Privacy Rule, it is no longer PHI, or subject to the HIPAA Rules, and, thus, may be used and disclosed by the covered entity or business associate for any purpose without restriction by HIPAA (but remains subject to any other applicable laws). The Privacy Rule designates **two ways whereby a covered entity can create de-identified health information**[71].

- **Breach Notification.** A "breach" is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the **unsecured protected health information**[72], such that the use or disclosure poses a significant financial risk or financial, reputational, or other harm to the affected individual. The **Breach Notification Rule**[73] specifies what is considered a breach, how and when these breaches must be disclosed, and what the penalties are. For instance, health care providers and their contractors must notify the patient, HHS, and the media in certain circumstances.

71 http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/deidentificationworkshop2010.html
72 http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html
73 The Breach Notification Rule is an interim final rule and subject to future final rulemaking.