HIPAA privacy and security toolkit:

Helping your practice meet new compliance requirements

These materials do not constitute legal advice and are for educational purposes only. The information in this packet is based on current federal law and subject to change based on changes in federal law, the effect of state law or subsequent interpretative guidance.

www.ama-assn.org/go/hipaa

AMA
AMERICAN MEDICAL ASSOCIATION

Table of Contents

Note: Some links in this resource will take you off the AMA website. The AMA is not responsible for the content of other websites.

How to “HIPAA” 2.0-Tip # 1: Understand the Basics

....

Understand the basics.

HIPAA is the acronym for the Health Insurance Portability and Accountability Act. Although HIPAA covers many things, physicians typically are most concerned with HIPAA’s Administrative Simplification provisions, and particularly the Privacy, Security and Breach Notification requirements. Since it was originally enacted, HIPAA has been amended and expanded several times as a result of new laws and regulations. The most sweeping change resulted from the Health Information Technology for Economic and Clinical Health Act (HITECH), enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA).

This toolkit provides an overview of the HIPAA Privacy, Security and Breach Notification Rules with which almost all physicians must comply. At their core, these rules simply implement longstanding physician commitments to protect the confidentiality of their patients’ medical information and maintain open physician-patient communications. However, the specificity of the requirements goes well beyond traditional, self-evident obligations, and violations can result in serious penalties. Thus, physicians need to understand these rules and participate in a formal compliance plan designed to ensure all the requirements are met. Physicians should also note that HIPAA is considered a “floor,” meaning, states may have requirements that go above and beyond what the federal government requires. This toolkit is focused on the federal mandates.

In a nutshell, these three core compliance areas include:

1. The Privacy Rule

The Privacy Rule restricts covered entities’ and business associates’ use and disclosure of an individual’s "protected health information" (PHI). Physicians who transmit PHI electronically in a HIPAA Standard Transaction, such as by filing electronic claims or checking eligibility electronically even if they are using a third party such as a billing service or a clearinghouse, are “covered entities,” and bound by HIPAA. “Business associates” include those persons and companies that physicians hire to help their practice and that have access to their patients’ PHI, such as billing services, attorneys, accountants and consultants. "Protected health information" means individually identifiable information that is held or transmitted by a covered entity or business associate in any form or media—whether electronic, paper, or oral, that relates to the past, present, or future physical or mental health of an individual, health care services, or payment for health care. The Privacy Rule also provides for “individual rights” such as a patient’s right to access their PHI, restrict disclosures, request amendments or an accounting of disclosures and their right to complain without retaliation.

2. The Security Rule

The Security Rule requires covered physician practices to implement a number of what are known as “administrative, technical, and physical safeguards” (described further on page 14) to ensure the confidentiality, integrity, and availability of *electronic* PHI. "Electronic PHI or *e*PHI" refers to all individually identifiable health information a covered entity or business associate creates, receives, maintains or transmits in electronic form. The Security Rule does not apply to PHI transmitted orally or in paper form.

3. The Breach Notification Rule

The Breach Notification Rule requires covered physician practices to notify affected individuals, the Secretary of the U.S. Department of Health & Human Services (HHS) and, in some cases, the media when they discover a breach of a patient's unsecured PHI.

Compliance deadlines

Most of these obligations took effect years ago, and thus most physician practices likely have established a HIPAA compliance plan. However, because changes to the physician practice will likely impact HIPAA obligations, such as the implementation of an EHR or participation in a health information exchange (HIE), or, because a new business associate agreement will be required, even just a change in billing services, physician practices are well advised to reevaluate and update their HIPAA compliance plans regularly to be sure they are meeting federal requirements. Indeed, the HIPAA Security Rule requires "periodic technical and non-technical evaluations". Moreover, HHS recently adopted new rules which make changes to existing privacy, security and breach notification requirements in what is often referred to as the final "HIPAA Omnibus Rule" implementing the HITECH Act. The HITECH Act is the same law that created the Electronic Health Records (EHRs) Incentive Program under Medicare and Medicaid. **All covered physician practices must update their HIPAA policies and procedures and otherwise implement the changes required by these regulations no later than the *September 23, 2013 compliance date.***

Government Audits

HHS is required to audit to ensure covered entities and business associates are complying with the HIPAA Privacy, Security and Breach Notification requirements. The HHS' Office of Civil Rights ("OCR"), the federal agency within HHS with oversight over HIPAA privacy, security and breach notification requirements, established a comprehensive audit protocol that physician practices may wish to consider as they review and update their HIPAA compliance plans. The OCR audit protocol contains 170 audit areas (79 Security Rule, 10 Breach Notification Rule and 80 Privacy Rule provisions) covering all of the following:

- Privacy Rule requirements for (1) notice of privacy practices for PHI, (2) rights to request privacy protection for PHI, (3) access of individuals to PHI, (4) administrative requirements, (5) uses and disclosures of PHI, (6) amendment of PHI, and (7) accounting of disclosures.
- Security Rule requirements for administrative, physical, and technical safeguards
- Breach Notification Rule requirements.

Physician practices may wish to review the OCR HIPAA audit protocol to serve as a checklist for their own compliance efforts. The AMA recognizes that this can be a daunting task, however, taking the time to do this will mitigate the impact of inappropriate release of and access to protected patient information and could help mitigate the impact of an audit on your practice. The protocol, which may be downloaded as an Excel spreadsheet, clearly indicates the audit procedure OCR has followed with respect to each key HIPAA compliance activity mandated by each regulatory provision. For example, with respect to business associate agreements as mandated by the federal government 45 CFR 164.504[1], the OCR protocol provides the following description of its audit procedure:

> Inquire of management as to whether a business associate contract permits the use and disclosure

[1] The OCR audit protocol includes references to the numbers of each regulation included in the HIPAA Privacy, Security and Breach Notification rules.

of PHI for the proper management and administration of the business associate. Obtain and review formal or informal policies and procedures related to business associate agreements. Obtain and review formal or informal policies and procedures and evaluate the content relative to the specified criteria for identifying whether a business associate agreement is required. Verify whether the agreement limits uses and disclosures to those that are permitted by the standard. Obtain and review a business associate agreement and evaluate the content relative to the specified criteria.

Similarly detailed descriptions are included for each of the 170 potential audit areas. While OCR is currently evaluating this protocol and may revise it, it nonetheless provides a good overview of the government's current enforcement priorities, and future versions will similarly provide helpful insight into the government's enforcement perspective. Thus, it should give you an idea of what the government is looking for when it comes to compliance.

How to "HIPAA" 2.0-Tip # 2: Know Your Compliance Requirements

....

Know your compliance requirements.

HIPAA: Who Must Comply?

Physicians who conduct any of the below named transactions electronically are required to comply with HIPAA:

- ASC[2] X12 837 Health Care Claim: Professional
- ASC X12 835 Health Care Claim Payment/Remittance Advice
- ASC X12 276 Heath Care Claim Status Request
- ASC X12 277 Health Care Claim Status Response
- ASC X12 270 Health Care Eligibility Benefit Inquiry
- ASC X12 271 Response
- ASC X12 278 Health Care Services Review Information - Review
- ASC X12 278 Health Care Services Review Information - Response
- ASC X12 837 Health Care Claim: Professional
- ASC X12 834 Benefit Enrollment and Maintenance
- ASC X12 820 Payment Order and Remittance Advice[3]

Physicians can also use a tool developed by the U.S. Department of Health & Human Services (HHS) if they are unclear whether or not they are a covered entity under HIPAA.

How to "HIPAA" 2.0-Tip # 3: Prioritize Your Compliance Activities

....

Prioritize your compliance requirements.

Understanding targets for compliance

- Federal law
- State law
- Regulatory changes and guidance
- Practice changes

Evaluate current office practices by conducting a gap analysis/risk assessment

- Compliance official – Has someone been given primary responsibility for HIPAA compliance – including the privacy, security and breach notification requirements?

[2] Accredited Standards Committee
[3] Standards for the Additional Information to Support a Health Care Claim or Encounter have not yet been adopted.

- Policies and procedures – Do your HIPAA policies and procedures reflect the realities of your current practice and meet the requirements of current law?

- Patient requests – Is there a documented policy and procedure to handle:

  - Medical Record Access, inspection and copy requests – wdhen a patient asks you to provide the opportunity to review or obtain a copy of the patient's medical records, especially requests for electronic PHI copies?

  - Disclosure restriction requests – when a patient asks you to limit sharing their medical information with other covered entities?

  - Amendment requests – when a patient asks you to make a change to the information in the patient's medical record?

  - Accounting of disclosure requests – when a patient asks for a list of everyone who has come in contact with the patient's record?

  - Confidential communication channel requests – when a patient requests to receive information in a specific way or at a specific location; for example they request to not be called at home for an appointment reminder?

- Notice of Privacy Practices (NPPs) – Does your practice maintain and share with your patients a Notice of Privacy Practices that clearly details how your practice will use and disclose PHI and your patients' rights, including their rights to prohibit the sale of their PHI or its use for marketing purposes, to request privacy protections and amendments to their PHI, to access their PHI, to receive notice of any breach and to obtain an accounting of disclosures? If your practice maintains a physical site (as opposed, for example, to being hospital-based), do you post the Notice of Privacy Practices in a prominent location? If your practice maintains a website, is your Notice of Privacy Practices posted on the website (also in a prominent location)? Read more about NPPs in the next section.

  - Training – Has all of your staff been trained to comply with your HIPAA policies and procedures? Do you periodically provide HIPAA Security training reminders?

  - Safeguards – Does your practice have the appropriate administrative, technical and physical safeguards to protect the privacy and security of your patients' PHI? Do these safeguards cover all of the appropriate requirements of the HIPAA Security rule?

  - Sanctions – Has your practice applied appropriate sanctions against members of the office workforce who have failed to comply with the HIPAA rules or your practice's privacy, security or breach notification policies and procedures?

  - Business associates – Has your practice entered into appropriate Business Associate Agreements with all of its agents that have access to PHI, to ensure that those agents also comply with all the HIPAA requirements?

  - Complaints – Is there a clear process for patients and staff to make complaints? Are complaints taken seriously? Has anyone who has complained suffered any retaliation?

- Breaches – Has the practice encrypted its PHI and otherwise taken all feasible steps to reduce the risk of breach? If a breach occurs, does the practice have appropriate policies for discovering and reporting the breach and mitigating any harm?

- Update your compliance plan and systems as necessary to close any gaps you have discovered.

    - Ensure all documentation is current.

    - Enhance your staff training systems to cover all physicians, other clinicians, and office staff, and ensure your compliance official(s) is up to the task.

    - Spend the money required to ensure adequate safeguards are in place for your current information systems and practice.

    - Recommit the practice to the heightened standards of trust and transparency demanded of a 21st century medical practice.

How to "HIPAA" 2.0- Tip # 4: Make Your Notice of Privacy Practices Meaningful

....

Make your Notice of Privacy Practices meaningful.

Physicians covered by HIPAA must provide to all patients with whom they have a direct treatment relationship a formal notice of the uses and disclosures of protected health information (PHI) that may be made by the physician or his/her employees and of the patient's rights and physician's legal obligations with respect to their PHI. This is called a Notice of Privacy Practices (NPP).

While some physician practices have seen the NPP as simply an administrative burden, that is a mistake. A carefully crafted NPP can actually be a valuable practice asset. By clearly laying out the practice's policies with respect to the use and disclosure of PHI and its commitment to protecting patients' rights, the practice has:

- Set the stage for an appropriate, practice specific training program,
- Created a powerful marketing tool demonstrating the value your practice places on patient confidentiality and welfare, and
- Developed an important piece of the practice's HIPAA compliance documentation, which not only meets a technical requirement, but also provides patients an understanding of how their PHI is used and disclosed and thus an opportunity to request restrictions, advise of alternate ways to communicate or to complain about HIPAA.

Content of Notice of Privacy Practices

The Notice must be written in plain language and contain all the following:

Header

The Notice must contain the following statement prominently displayed:

"THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."

How the Physician Will Use and Disclose PHI

The Notice must include a series of specific statements relevant to the practice's use and disclosure of PHI, including when the patient's authorization will be required. If the physician practice is in a state that has laws that are more protective of patients' rights than HIPAA, the NPP must be consistent with those more stringent requirements.

Individual Rights

The Notice must contain a statement of the individuals' rights with respect to PHI and a brief description of how the individual may exercise those rights.

Physician's Duties

The Notice must include the physician's various duties under the HIPAA Privacy Rule, including the duty to abide by the practice's current NPP.

Complaints

The Notice must state that patients may complain to the physician or to the Secretary of HHS if they believe their privacy rights have been violated. A brief description of how to file a complaint and that there will be no retaliation must also be included.

Contact

The Notice must contain the name or title and telephone number of the person (generally the practice's designated privacy officer) to contact for further information.

Effective Date

The Notice must contain the date on which the notice is first in effect.

Optional Elements

The physician practice may include, and will be bound by, any additional, voluntary limitations on its use or disclosure of PHI, provided it may not limit uses or disclosures required by law or the right, to the extent it is otherwise permitted by law and standards of ethical conduct, to disclose information the physician believes in good faith is necessary to prevent or lessen a serious and unwarranted threat to the health or safety of a person or the public.

Sample Notice of Privacy Practices

The AMA's sample Notice of Privacy Practices designed for a typical physician office and updated to reflect the requirements of the Omnibus rule is available.

Physicians must promptly revise their Notice of Privacy Practices (NPPs) whenever there is a material change to the uses or disclosures, the patient's rights, the physician's legal duties, or other privacy practices stated in the Notice.

Amendments to NPPs required by the recent HIPAA Omnibus Rule include those related to breach notification, disclosures to health plans, and marketing and sale of PHI. To the extent physicians engage in fundraising, they will also have to amend their NPP to inform patients of their right to opt-out of those communications. The new rules also eliminate requirements to include information on communications concerning appointment reminders, treatment alternatives or health-related benefits or services in NPPs, but the rules do not require that that information be removed either.

Providing the Notice

Physicians who have a direct treating relationship with their patients (as opposed to physicians who may only do diagnostic studies in a hospital setting and never see the patient) are required to provide the Notice to new patients and use their best efforts to obtain acknowledgment of receipt. While physicians are free to provide email copies or have patients review a laminated copy, the rules require that physicians make a hard copy version available to those patients who want to take a copy with them.

As the rules presume all the amendments discussed above are material changes, physicians will have to post the revised NPP, and make copies available at their office, to all new patients and to anyone else on request. Physicians who maintain a website are cautioned to post the updated NPP on their website as required by the existing HIPAA Privacy rule.

How to “HIPAA” 2.0-Tip # 5: Understand the Breach Notification Rule

....

Understand the Breach Notification Rule.

Physicians who are covered by HIPAA have been required to notify patients if there are breaches of security involving their medical information for some time.

The HIPAA Omnibus rule, effective September 23, 2013, expanded and clarified this obligation. As a result, physicians must update their HIPAA breach notification policies and procedures.

Under the new rules, breaches are now presumed reportable unless, after completing a risk analysis applying the following four factors, it is determined that there is a “low probability of PHI compromise.” The four factors to be considered include:

- The nature and extent of the PHI involved – issues to be considered include the sensitivity of the information from a financial or clinical perspective and the likelihood the information can be re-identified;
- The person who obtained the unauthorized access and whether that person has an independent obligation under HIPAA to protect the confidentiality of the information;
- Whether the PHI was actually acquired or accessed, determined after conducting a forensic analysis; and
- The extent to which the risk has been mitigated, such as by obtaining a signed confidentiality agreement from the recipient.

This rebuttable presumption of breach and four-factor assessment of the “risk of PHI compromise” replaces a previous, more subjective “significant risk of financial, reputational or other harm” analysis for establishing a breach. The new rules further clarify that there is no need to have an independent entity conduct the risk assessment and indeed, no risk assessment need be conducted at all if the breach notification is made (although, physicians will want to undertake an appropriate review and steps to mitigate the harm and reduce the likelihood of future breaches in any case). The new rules further confirm that the breach notification requirement may be delegated to a business associate (BA), and physicians are encouraged to coordinate with their BAs so that patients receive only one notification of the breach.

Learn more about conducting a general security risk analysis, which you should do in conjunction with any breach to reduce the risk of future breaches.

The new rules do not modify the actual reporting and timeframe requirements for Breach Notification; that is, covered entities must still adhere to requirements for individual notification, HHS notification and, where applicable, media posting of the breach. Also the new rules do not modify the definition of unsecured PHI—that is, PHI that has not been properly secured. Electronic PHI that is encrypted is secured, and thus not subject to the breach notification requirements. For more information on breach notification requirements see the AMA’s fact sheet. View “HIPAA Security Rule: Frequently asked questions regarding encryption of personal health information” for more information on how to encrypt *e*PHI.

How to “HIPAA” 2.0-Tip # 6: Evaluate Your Business Associates

....

Evaluate your Business Associates.

The HIPAA Privacy Rule generally prohibits covered physicians from using or disclosing PHI except pursuant to a written authorization signed by the patient or for treatment, payment or health care operations (i.e., quality reporting). However, covered physicians can disclose PHI to their "business associates" and authorize them to create, maintain or receive PHI on their behalf, if they take specified steps to safeguard the information, including the execution of a written Business Associate agreement (BAA).

Initially, the law defined “Business Associates” to be all those persons or entities who, on behalf of the physicians:

- Perform or assist in the performance of any function or activity that involves the use or disclosure of PHI, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, re-pricing or any other function or activity regulated by the Administrative Simplifications Provisions of HIPAA; and

- Provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services that involve PHI.

The new HIPAA Omnibus rules expand the universe of individuals and companies which must be treated as business associates to include Patient Safety Organizations (PSOs) and others involved in patient safety activities, health information organizations like e-prescribing gateways, or health information exchanges that transmit and maintain PHI and personal health record vendors physicians sponsor for their patients. The new rule also clarifies that some organizations with “persistent” access to PHI they maintain (such as a document storage firm or a data center that provides hosting or ePHI backup) are also business associates. Thus, physicians must review their relationships and determine if they must enter into new BA agreements with these entities or others that create, receive, store, maintain or transmit PHI on their behalf. One way to think of this is if an organization or individual with whom you do business has access to your patient’s protected health information. then there is a strong likelihood that you need to have a BAA with them.

These rules also modify the requirements for BA agreements:

- Physicians no longer must report failures of their BAs to the government when termination of the BAA is not feasible, since the government has concluded that the BA’s direct liability for these violations is sufficient;
- BAs are now responsible for their subcontractors;
- BAs must comply with the Security and Breach Notification Rules; and
- Physicians are liable for the actions of their BAs who are “agents,” but not for the actions of those BAs that are “independent contractors.” Physicians will need expert legal assistance to determine whether a particular BA is an agent or an independent contractor; as a general matter, the difference depends on the amount of control the physician retains to direct the BA’s actions – the more authority the physician retains to direct how the BA accomplishes the contracted responsibility, the more likely the BA will be considered an agent, for which the physician will retain liability.

AMA's sample BA agreement has been revised to include these new requirements.

Physicians have until September 23, 2014, to bring all their BA agreements into conformance with the new rules. BA agreements that have not been renewed or modified between March 26, 2013, and September 23, 2013, will be deemed compliant until the date the BA agreement is renewed or modified or until September 22, 2014, whichever is earlier.

How to “HIPAA” 2.0-Tip # 7: Understand the HIPAA Security Rule

....

Understand the HIPAA Security Rule.

The HIPAA Security Rule requires physician practices to implement a number of administrative, technical, and physical safeguards to ensure the confidentiality, integrity, and availability of *electronic* PHI.

"Electronic PHI" refers to all individually identifiable health information a covered entity or business associate creates, receives, maintains or transmits in electronic form. The Security Rule does not apply to PHI transmitted orally or in paper form.

The goals of the security rules are to ensure the confidentiality, integrity and availability of all electronic protected health information (*e*PHI), and to protect against anticipated disclosures and threats to the security of the information. They incorporate the concepts of scalability, flexibility and generalization. In other words, the regulations do not expect the same security precautions from small or rural providers as are demanded of large covered entities, such as those in urban centers, with significant resources. Security is recognized as an evolving target, and so the federal government employed generalized security requirements that are not linked to specific technological advances. "[W]e have focused more on what needs to be done and less on how it should be accomplished," states HHS.

The final regulations are divided into "required" and "addressable" standards. While the "required" standards are just that, the "addressable" standards may be mandatory as well. Covered entities must assess how reasonable and appropriate implementing the "addressable" standards would be, and do so where appropriate. Where an "addressable" standard would be inappropriate, a covered entity may instead adopt an alternate means to the same end or possibly forgo the proposal altogether. But HHS has made it clear that cost alone is not a sufficient basis for declining adoption of a standard. For example, if adoption of secure email and messaging were costly, this would not exempt a physician from using a secure method of emailing PHI, should they choose to want to email PHI.

Connection to the Privacy Regulations

It can be easy to confuse what the Privacy Rule aims to do with what is required under the Security Rule. They are different but complementary sets of requirements under HIPAA and are considered inextricably linked. While the Privacy requirements apply to any form of protected health info (paper and electronic), the Security Rule only applies to data that is in an electronic form. The Privacy Rule sets forth the requirements for ensuring patient’s information stays private by regulating the use and disclosure of any form of PHI, whereas the Security Rule outlines the types of security safeguards that are need to protect information in an electronic form (ePHI). HHS notes that compliance with privacy standards will, in many instances, account for a substantial step towards security compliance.

An exception to this overlap is found in the "scope of information" covered by the security regulations compared to privacy, as pertaining to physicians. While the privacy regulations involve all protected health information (PHI) no matter what the form, the security rules covers only *electronic* PHI. Physicians will find, however, that other, non-electronic PHI may require security protections under the privacy rules. As was the case with the privacy regulations, "business associates" and hybrid entities also have duties under the security rules.

Risk Assessment

Covered entities must assess their security risks. This is the foundation of compliance. Risk assessment is tailored to the covered entity—its size, complexity and capabilities, in addition to risk and cost, are all taken under consideration when determining whether an "addressable" standard applies or how to best meet a "required" standard. The rules are not prescriptive—a number of different tactics can achieve compliance. These same factors listed above are to be considered when determining an entity's appropriate response.

Conducting a HIPAA Security Risk Analysis or Assessment is also a Core Objective to reach “meaningful use” of a Certified Electronic Health Record, enabling you to receive incentives and avoid Medicare penalties.

Once a physician / practice has identified where PHI is stored and moved electronically, they must determine if any of these places are at risk for not having appropriate safeguards for protecting ePHI (aka “vulnerabilities”). Meaning, where are the places in your practice where ePHI could be vulnerable to access not allowed under HIPAA and what are you doing to ensure patient’s data is protected? The physician / practice should then turn their attention to addressing any identified vulnerabilities in order to reduce their risks of a breach.

The Big Three—The Components of the Security Standards

"Administrative safeguards" focus on workforce training and contingency planning (45 CFR §164.308). The cornerstones, however, are risk analysis and risk management—both "required." Critical and thorough risk analysis must take place before any attempt at regulatory compliance is made.

Additional "required" administrative safeguards include:

- Sanctions for workforce noncompliance.
- Tracking of security "incidents," and documented policies and procedures for dealing with incidents. Resulting harm must be mitigated.
- Appointment of a single security officer—this person could well be the privacy officer too.
- Allowing workforce access to ePHI only where appropriate, and putting policies in place to prevent unauthorized persons from gaining access.
- Training workforce on security issues, scaled to the organization. Covered entities must train their staffs in security in an ongoing fashion—a single session will not be sufficient. "Business Associates" must be aware of security policies, though the covered entity is not under an obligation to train the associates.
- Contingency plans for emergencies that damage systems with ePHI, including provisions for data backup, a recovery plan and a mode for continuing critical business processes for the protection of the security of ePHI during emergency operation.
- Periodic evaluations of security preparedness, conducted either internally or externally.

"Physical safeguards" are concerned with access both to the physical structures of a covered entity and its electronic equipment (45 CFR §164.310). *e*PHI and the computer systems upon which it resides must be protected from unauthorized access, in accordance with defined policies and procedures. Some of the requirements under the physical safeguards heading can be accomplished through the use of electronic security systems.

"Required" physical safeguards include:

- Establishing policy for the appropriate use, physical attributes of and security for workstations that access ePHI.
- Establishing policies dictating procedures for the addition, disposal or reuse of hardware or electronic media that contains ePHI.

"Technical safeguards" may be the most difficult part of the security regulations to comprehend and implement for those lacking technical savvy.

"Required" technical safeguards include:

- Establishing policies limiting software program access to only those with authorized access. Unique log-ins, either numeric or by name, are required—automatic log-offs are not. Procedures for obtaining necessary *e*PHI during an emergency are also required.
- Activity logs ("audit logs") of all systems that contain *e*PHI must be maintained.
- Policies to protect *e*PHI from alteration and destruction must be established.
- Procedures as required to verify the identity of those seeking access to *e*PHI must be maintained.
- Transmission of *e*PHI over a network must be protected by technical security policies. Encryption is an "addressable" standard; however, in light of the breach notification requirements, encryption is increasingly a practical necessity. Learn more by accessing the AMA's resource, "HIPAA Security Rule: Frequently asked questions regarding encryption of personal health information."

Each of the three categories above contains additional "addressable" safeguards that may or may not be applicable to your organization. A proper risk assessment will inform you of any further obligations.

Document! Document! Document!

Behind every security compliance measure is a documentation requirement. Practically each facet of compliance requires that policies and procedures be created and implemented. Compliance activities must be documented and retained for six years. Documentation is a major part of the compliance battle and having policies in place will help you weather an audit.

Policies are amendable at any time, so long as documentation is also updated. The security regulations require periodic review of policies, and appropriate responses to changes in the environmental security of *e*PHI—as are deemed reasonable for the particular covered entity.

How to "HIPAA" 2.0-Tip # 8: Know Your Patient's Rights

....

Know your patient's rights.

The HIPAA Privacy Rules give patients a number of rights with respect to their personal health information (PHI). These rights, which should all be documented in the physician practice's Notice of Privacy Practices, include:

- The right to inspect and copy PHI.
- The right to amend PHI.
- The right to request restrictions on certain uses and disclosures of PHI, including to request that a health plan not be informed of treatment for which the patient paid entirely out of pocket (as described in more detail below).
- The right to receive confidential communications of PHI "by alternative means or at alternative locations."
- The right to prohibit the sale of their PHI, its use for marketing purposes, or participation in research.
- The right to receive an accounting of disclosures of PHI, that is, a list of those third parties who have been given access to the patient's PHI.
- The right to complain about a HIPAA privacy violation.

The HIPAA Omnibus rule will likely require changes to a physician practice's HIPAA policies and procedures relevant to these rights in at least the following areas:

- **Disclosures to health plans** – At the patient's request, physicians generally may not disclose information about care the patient has paid for out-of-pocket to health plans. This change updates the previous HIPAA Privacy Rule governing patient requests for restrictions on the use or disclosure of their PHI. While previously physicians could refuse to abide by any such request, the new rule *requires* physicians and other health care providers to abide by a patient's request not to disclose PHI to a health plan for those services for which the patient has paid out-of-pocket and requests the restriction. Of all the changes made by the new rules, this change is likely to have the greatest impact on your practice workflow both in terms of documentation and follow up to ensure the restriction is adhered to.

- **Marketing communications** – The new rules further limit the circumstances when physicians may provide marketing communications to their patients in the absence of the patient's written authorization. Generally speaking, the only time a physician may tell a patient about a third-party's product or service without the patient's written authorization is when: 1) the physician receives no compensation for the communication; 2) the communication is face-to-face; 3) the communication involves a drug or biologic the patient is currently being prescribed and the payment is limited to reasonable reimbursement of the costs of the communication (no profit); 4) the communication involves general health promotion, rather than the promotion of a specific product or service; or 5) the communication involves government or government-sponsored programs. Physicians are still permitted to give patients promotional gifts of nominal value.

- **Sale of PHI** – The new rules clarify that the prohibition on the sale of PHI in the absence of the patient's written authorization also now includes situations involving agreements to license or lease access to PHI as well as an outright sale, and to the receipt of financial or in-kind benefits in exchange for PHI. It also includes disclosures in conjunction with research if the remuneration received includes any profit margin. On the other hand, the prohibition on PHI sales does not extend to otherwise permitted disclosures for payment or treatment, nor to permitted disclosures to patients or their designees in exchange for a reasonable cost-based fee. In other words, sending a claim to an insurer for payment for services rendered to a patient is not considered part of the "sale" definition.

- **Copies of *e*PHI** – Physicians will now have only 30 days to respond to a patient's written request for his or her PHI with one 30-day extension, regardless of where the records are kept (eliminating the longer 60-day timeframe for records maintained offsite). They must provide access to EHR and other electronic records in the electronic form and format requested by the individual if the records are "readily reproducible" in that format. Otherwise they must provide the records in another mutually agreeable electronic format. Hard copies are permitted only when the individual rejects all readily reproducible *e*formats. Physicians must also consider transmission security, and may send PHI in unencrypted emails only if the requesting individual is advised of the risk and still requests that form of transmission.

- **Charging for copies of ePHI or PHI** – The new rule modifies the costs that may be charged to the individual for copies to include labor costs (potentially to include skilled technical labor costs for extracting electronic PHI) and supply costs if the patient requests a paper copy, or if electronic, the cost of any portable media (such as a USB memory stick or a CD), assuming state law does not set a lower reimbursement rate. The rule also clarifies that physicians may impose a separate charge for creating an affidavit of completeness.

- **Research authorizations** – The new rules permit physicians to combine conditioned and unconditioned authorizations for research participation, provided individuals can opt-in to the unconditioned research activity. Moreover, these authorizations may encompass future research.

How to "HIPAA" 2.0-Tip # 9: Really Limit Disclosures of PHI to the Minimum Necessary

....

Really limit disclosures of PHI to the minimum necessary.

Physicians are generally required by HIPAA to make reasonable efforts to limit protected health information (PHI) to the "minimum necessary" to accomplish the intended purpose of the use, disclosure or request. OCR has explained its interpretation of the minimum necessary requirement as follows:

> The minimum necessary standard, a key protection of the HIPAA Privacy Rule, is derived from confidentiality codes and practices in common use today. It is based on sound current practice that protected health information 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's requirements for minimum necessary are designed to be sufficiently flexible to accommodate the various circumstances of any covered entity.

Given the fact that a violation of the "minimum necessary" requirement may trigger the breach notification requirements, physicians should ensure that the minimum necessary requirement is met.

Since February 17, 2010, the Health Information Technology for Economic and Clinical Health (HITECH) Act has required HIPAA-covered physicians to use, disclose, or request only the ***limited data set*** to the extent that is adequate to accomplish the intended purpose of that use, disclosure or request (this may be modified when the final guidance on what constitutes "minimum necessary" is published). Moreover, the party disclosing the PHI determines what constitutes the minimum necessary to accomplish the intended purpose of the disclosure.

Limited Data Set Defined

To be a "limited data set" the PHI *must not include any of the following identifiers* of the individual and any relatives, employers or household members of the individual:

- Names;
- All geographic subdivisions smaller than a State other than town or city and zip code, including street address or precinct;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;

- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code, except as permitted by the regulation (45 C.F.R. §164.514(c)) to allow the data to be re-identified by the sender.

Essentially, a "limited data set" is the same as fully de-identified information except it may contain town or city and zip code, and dates directly related to an individual, including birth date, admission date, discharge date, age and date of death.

Exceptions to Applications of Minimum Necessary Rule

The minimum necessary rule does not apply to the following circumstances:

- 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 written authorization;
- Uses or disclosures that are required by law; and
- Uses or disclosures required for compliance with the HIPAA Privacy Rule, or to HHS pursuant to a HIPAA investigation or compliance review.

Policies and Procedures on Requesting or Releasing PHI

Physicians must adopt policies and procedures governing (1) requests for PHI and (2) disclosures of PHI as follows:

Routine requests or disclosures – physicians must implement policies and procedures that limit the PHI requested or disclosed to that "reasonably necessary to achieve the purpose."

Ad hoc requests or disclosures – physicians must develop criteria designed to limit the request or disclosure to the minimum necessary, and review such requests or disclosures on an individual basis in accordance with these criteria.

Reliance on Representations on what constitutes Minimum Necessary

The HIPAA Privacy Rule permits physicians to rely on the judgment of the requesting party as to the minimum amount of information that is needed under certain circumstances. Such reliance must be reasonable under the particular circumstances of the request. Such reliance is allowed when the request is made by:

- A public official or agency that is authorized to access the information and states that the information requested is the minimum necessary for the stated purpose.

- A health plan, health care clearinghouse, or other health care provider covered by HIPAA, or a professional who is a workforce member or business associate of a health plan, clearinghouse or covered health care provider who requests the information for the purpose of providing professional services to that covered entity, and states that the information requested is the minimum necessary for the stated purpose.

- A researcher with appropriate documentation from an Institutional Review Board (IRB) or Privacy Board.

Caution: The HIPAA Final Omnibus Rule modifies the current minimum necessary standard so that it now applies directly to business associates as well as covered entities. However, further changes could be made when the final guidance on the minimum necessary requirement are issued, as the HITECH Act amended the law to require that the "covered entity or business associate disclosing the PHI determines what constitutes the minimum necessary to accomplish the intended purpose of the disclosure."

How to “HIPAA” 2.0-Tip # 10: Beware of Significant Penalties

....

Beware of the significant penalties.

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

Civil Penalties

The HITECH Act established a tiered civil penalty structure for HIPAA violations (see below). The Secretary of the Department of Health and Human Services (HHS) still has discretion in determining the amount of the penalty based on the nature and extent of the violation and the nature and extent of the harm resulting from the violation. The Secretary is still prohibited from imposing civil monetary penalties (CMPs) (except in cases of willful neglect) if the violation is corrected within 30 days (this time period may be extended). Furthermore, HHS may waive a CMP in whole or in part in some situations. And, HHS' authority to impose a civil money penalty is prohibited if a criminal penalty (as described in greater detail below) has been imposed.

HIPAA Violation	Penalty Range	Annual Maximum
Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA	$100 - $50,000 per violation	$1.5 million
Individual “knew, or by exercising reasonable diligence would have known” of the violation, but did not act with willful neglect	$1,000 - $50,000 per violation	$1.5 million
HIPAA violation due to willful neglect but violation is corrected within the required time period	$10,000 - $50,000 per violation	$1.5 million
HIPAA violation is due to willful neglect and is not corrected	$50,000 per violation	$1.5 million

Pursuant to the HIPAA Omnibus Rule, HHS must conduct a formal investigation and impose civil monetary penalties in cases involving willful neglect, and is now free to provide PHI to other government agencies for enforcement activities. The assessment of penalties must be based on five principal factors: (1) the nature and extent of the violation, including the number of individuals affected, (2) the nature and extent of the harm resulting from the violation, including reputational harm, (3) the history and extent of prior compliance, (4) the financial condition of the covered entity or business associate, and (5) such other matters as justice may require. The number of violations may be based on the number of individuals affected or by the number of days of non-compliance. Finally the Omnibus rule clarifies that the 30-day cure period begins when the individual knew or should have known of the violation.

Criminal Penalties

Covered entities and specified individuals, as explained below, whom "knowingly" obtain or disclose individually identifiable health information in violation of the HIPAA requirements face a fine of up to $50,000, as well as imprisonment up to one year. Offenses committed under false pretenses allow penalties to be increased to a $100,000 fine, with up to five years in prison. Finally, offenses committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain or malicious harm permit fines of $250,000, and imprisonment for up to ten years.

- **Covered Entity and Specified Individuals**
  The DOJ concluded that the criminal penalties for a violation of HIPAA are directly applicable to covered entities—including health plans, health care clearinghouses, health care providers who transmit claims in electronic form, and Medicare prescription drug card sponsors. Individuals such as directors, employees, or officers of the covered entity, where the covered entity is not an individual, may also be directly criminally liable under HIPAA in accordance with principles of "corporate criminal liability." Where an individual of a covered entity is not directly liable under HIPAA, they can still be charged with conspiracy or aiding and abetting.
- **Knowingly**
  The DOJ interpreted the "knowingly" element of the HIPAA statute for criminal liability as requiring only knowledge of the actions that constitute an offense. Specific knowledge of an action being in violation of the HIPAA statute is not required.
- **Full DOJ memorandum**
  Read the full DOJ memorandum here.
- **Exclusion**
  The Department of Health and Human Services (HHS) has the authority to exclude from participation in Medicare any covered entity that was not compliant with the transaction and code set standards by October 16, 2003 (where an extension was obtained and the covered entity is not small) (68 FR 48805).
- **Enforcing Agencies**
  The HHS Office of Civil Rights (OCR) enforces the privacy and security rules, while the Centers for Medicare & Medicaid Services (CMS) enforces the transaction and code set standards.
- **No Private Cause of Action**
  While HIPAA protects the health information of individuals, it does not create a private cause of action for those aggrieved (meaning an individual cannot take legal action against a covered entity for a HIPAA violation based on the HIPAA law). State law, however, may provide other theories of liability.

How to "HIPAA" 2.0-Tip # 11: Look to the AMA and Website Resources for Updates

....
Look to the AMA and website resources for updates.

The HIPAA Privacy, Security and Breach Notification rules continue to be revised, and technological change continues to impact the application of those rules. Physician practices must ensure they stay on top of these changes to protect their patients' rights, maintain compliance and avoid the potentially draconian penalties for violations.

American Medical Association HIPAA information

AMA provides a host of information designed to help physicians comply with the HIPAA Privacy, Security and Breach Notification Rules.

http://www.ama-assn.org/go/HIPAA

US Department of Health and Human Services (DHHS) Office of Civil Rights (OCR)

The HHS OCR website contains a wealth of information on the HIPAA Privacy and Security Rules, including a list serv and a link to the Transaction and Code Sets information posted by CMS.

http://www.hhs.gov/ocr/privacy/index.html

Centers for Medicare and Medicaid Services (CMS)

This link to the CMS website includes information on the Transaction and Code Sets Rule.

http://www.cms.gov/Regulations-and-Guidance/Regulations-and-Guidance.html

Workgroup for Electronic Data Interchange (WEDI)

This is the WEDI website which includes information on EDI in the health care industry, lists of conferences, implementation information and the availability of resources for standard transactions.

http://www.wedi.org

National Committee on Vital and Health Statistics (NCVHS)

This is the NCVHS website. NCVHS is the Advisory Body to the Department of Health and Human Services responsible for the HIPAA Transaction and Code Set Rule. Information on membership, how to contact the committee, announcements and agendas for past and future public hearings is also available.

http://www.ncvhs.hhs.gov

Medicare

This is the Medicare EDI Web page. Here you will find information regarding Medicare EDI, advantages to using Medicare EDI, Medicare EDI formats and instructions, news and events, frequently asked questions about Medicare EDI, and information regarding Medicare paper forms and instructions.

http://www.cms.gov/Medicare/Billing/ElectronicBillingEDITrans/index.html