From the Author

Of the ten books I’ve written, this is certainly the shortest. I am hopeful it will be one of the most beneficial.

My goal is simple: Provide an easy-to-understand resource for answering the most common patient privacy questions.

My thanks to my friends and colleagues at Smart Training LLC for their support and guidance.

Remember that there is no “wise old man” with respect to patient privacy. Like this book, HIPAA compliance is a work in progress.

If you have questions or comments, feel free to email me:

jimmoore@smarttrainingllc.com
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section 1</td>
<td>General Information About HIPAA</td>
<td>4</td>
</tr>
<tr>
<td>Section 2</td>
<td>Understanding the HIPAA Privacy Rule</td>
<td>7</td>
</tr>
<tr>
<td>Section 3</td>
<td>Questions About PHI Disclosures</td>
<td>17</td>
</tr>
<tr>
<td>Section 4</td>
<td>Privacy Officers and Administrative Requirements</td>
<td>18</td>
</tr>
<tr>
<td>Section 5</td>
<td>About Physical and Technical Safeguards</td>
<td>20</td>
</tr>
<tr>
<td>Section 6</td>
<td>Strategies to Protect Electronic PHI</td>
<td>22</td>
</tr>
</tbody>
</table>
Section One: General Information About HIPAA

1. What the heck is HIPAA, anyway?

As you might expect, I’ve frequently had harrassed new healthcare employees ask me this question. I’ve heard other employees jump in and answer, “That’s those forms we give patients when they first come in.” Well, that’s a good answer, but it’s not exactly the whole story. Let’s start from the top:

HIPAA is an acronym.

The Health Insurance Portability and Accountability Act was passed by Congress in 1996, during the Clinton administration. Many conservative healthcare professionals like to blame all their compliance woes on Democrats like Bill Clinton, but the truth is something else: The actual groundwork for patient privacy law was laid during the Bush administration several years earlier.

There are substantial parts of HIPAA that you don’t think about nowadays. The law provides millions of American workers and families with the ability to transfer and continue their health insurance coverage when they lose or change jobs. HIPAA was also created to reduce healthcare fraud and waste. The law mandates industrywide standards for health care information that appears on electronic billing and other processes. Additionally, HIPAA requires that Protected Health Information, or PHI, be protected and handled in a confidential manner. This requirement is the reason for this book ... and for harrassed practice employees to wonder what HIPAA is in the first place.

Like all Federal law, HIPAA is divided into subtitles. The one section (of five) which addresses patient privacy standards and affects the majority of healthcare organizations is known almost comically as “Administrative Simplification.” As you will see, there’s almost nothing simple about HIPAA.

2. What businesses must comply with HIPAA?

Healthcare operations called “Covered Entities” are bound by HIPAA privacy standards. A “Covered Entity” may be a health plan, healthcare clearinghouse or healthcare providers who conduct certain financial and administrative transactions electronically.
3. **So how does the law define a healthcare provider?**

The law defines a healthcare provider as a trained, licensed provider of medical or health services who transmits HIPAA-identified standard transactions electronically. All physicians, dentists and chiropractors who transmit patient information electronically fit the definition of a healthcare provider.

4. **How does HIPAA define a health plan?**

The law defines a health plan as an individual or group that provides or pays the cost of medical care. Health plans can include:

- Health insurance carriers
- Group health plans
- HMOs – Health Maintenance Organizations
- Medicare (Part A or B)
- Medicare supplemental insurance policy issuers
- Long-term care policy issuers
- An employee arrangement offering or providing health benefits to employees of several employers
- Healthcare programs for active military personnel
- Veteran’s healthcare program
- CHAMPUS – the Civilian Health and Medical Program of the Uniformed Services
- The Indian Health Service program
- The Federal Employees Health Benefit program
- State-approved child health plans
- Medicare + Choice program
- State high-risk pools providing health insurance coverage to eligible individuals
- Any other individual or group plan providing or paying for the cost of medical care

5. **How does HIPAA define a healthcare clearinghouse?**

Under HIPAA, a healthcare clearinghouse is a Covered Entity that processes or facilitates processing of information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction. A healthcare clearinghouse would typically receive a standard transaction from another entity and process or facilitate the processing of health information into nonstandard format or nonstandard data content for the receiving entity.
6. **What are the standard transactions identified by HIPAA?**

Under HIPAA, standard electronic transactions between a healthcare practice and a health insurer include:
- Claims
- Explanation of Benefits or Remittance Advice
- Claim status request
- Claim status response
- Patient eligibility request
- Patient eligibility response
- Authorization request
- Authorization response
- Coordination of benefits
- Claims attachments
- First report of an injury

Standard electronic transactions between an insurance purchaser and a health insurer might include:
- Membership enrollment
- Premium payments
- Coordination of benefits

7. **Does HIPAA grant individuals the right to control their PHI?**

Yes. Under HIPAA, Federal privacy regulations grant individuals the right to be informed about and to control their Protected Health Information. This means that individual patients have the right to access and copy PHI, request an amendment to their PHI, receive an accounting of disclosures of their PHI, receive a notice of privacy practices, request restrictions on certain uses and disclosures of their PHI, and request that communication about their PHI be conducted in a confidential manner.

8. **Which takes precedence – State law or HIPAA?**

State laws that are contrary to the Privacy Rule are preempted by Federal requirements, unless a specific exemption applies. Only State laws that are contrary to Federal requirements can justify an exemption.

If the State law provides greater privacy rights or protections, provides for reporting of disease, injury, child abuse, births and deaths or requires certain health plan reporting, the State law preempts HIPAA requirements.

Generally, if a State law is more protective of the patient, that law takes precedence over HIPAA.
9. Are there cases in which more stringent State laws do not supercede HIPAA?

As we’ll see, the HIPAA Privacy Rule establishes a base level of Federal privacy protections and rights for individuals. In the few cases where a “more stringent” State law runs contrary to a provision of the Privacy Rule, the Administrative Simplification Rules specifically provide an exception to preemption of State law. HIPAA Administrative Simplification Rules exempt more stringent, contrary State law from preemption.

The Department of Health and Human Services may, upon specific request from a State or other entity or person, determine that a provision of State law which meets certain requirements but is “contrary” to the Federal requirements – as defined by the HIPAA Administrative Simplification Rules – will not be preempted by the Federal requirements.

The “certain requirements” are usually only those designed to prevent fraud or abuse, ensure appropriate State regulation of insurance and health plans, facilitate State reporting on healthcare delivery or cost, or serve some other “compelling need” relating to public health, safety and welfare.

10. Who actually enforces HIPAA?

HIPAA Privacy and Security Rules are enforced by the Office for Civil Rights, operating within the Department of Health and Human Services.

Section Two: Understanding the HIPAA Privacy Rule

11. What was the Privacy Rule originally designed to protect?

The Privacy Rule was written to protect “individually identifiable health information” held or transmitted by a Covered Entity or its Business Associate, in any form or media, whether electronic, paper or oral. The Privacy Rule calls this information “Protected Health Information,” or PHI.

“Individually identifiable health information” can include demographic data. More specifically, this information relates to the individual’s past, present or future physical or mental health or condition, the provision of health care to the individual, or the past, present or future payment for the provision of health care to the individual. The information also identifies the individual or can likely be used to identify the individual.

Here’s the important point to remember: “Individually identifiable health information” includes common identifiers like the patient’s name, address, birth date, Social Security Number, etc.

Excluded from Protected Health Information are employment records that a Covered Entity maintains in its capacity as an employer, as well as education and certain other records that are subject to or defined by the Family Educational Rights and Privacy Act.

12. When can a Covered Entity use and disclose PHI?

A Covered Entity is permitted, but not required, to use and disclose Protected Health Information without the individual’s authorization to the individual himself or herself, and for uses that meet what we call “the T-P-O Standard.” This means the information is used specifically to facilitate treatment, payment for treatment rendered or health care operations, when an opportunity to agree or object is offered.
An opportunity to agree or object might be offered when an individual is being listed in a facility patient directory or for notification purposes, incident to or adjacent to an otherwise permitted use or disclosure, and for activities that serve or benefit the public interest, as well as a Limited Data Set for the purposes of research, public health or health care operations.

13. Can you offer a more extensive definition of the TPO Standard?

I’ll try. To review: PHI can be shared with another health care entity without patient authorization or approval if the information is used to receive treatment, receive payment, or to facilitate healthcare operations. These treatment, payment and healthcare operations are typically referred to as “TPO.”

Treatment is usually defined as the provision, coordination or management of healthcare and related services by one or more healthcare providers, including coordination or management of healthcare by a provider and consulting between healthcare providers relating to a patient or the referral of a patient for healthcare from one health care provider to another.

Payment usually refers to activities related to an individual patient for whom healthcare or payment for healthcare is provided, in order to obtain or provide reimbursement for providing healthcare. Payment includes billing, claims management, collection activities, obtaining payment under a contract for reimbursement and related healthcare data processing, as well as review of healthcare services with respect to medical necessity, coverage under a health plan, appropriateness of care or justification of charges. Utilization-review activities, like pre-certification and pre-authorization of services and concurrent or retrospective review of services are also considered part of the payment dynamic.

Healthcare Operations of a Covered Entity can include conducting quality assessments and coordinating quality improvement activities, population-based activities related to improving health or reducing healthcare costs, conducting or arranging for medical review, legal services and auditing functions including fraud and abuse detection and compliance programs, and business management and general administrative activities. These can include managing HIPAA compliance, providing data analysis and resolving client disputes relating to quality of care or eligibility for service.

14. When must Covered Entities limit PHI use and disclosure?

This is a challenging question, made so because the concept of “minimum necessary” use and disclosure is central to the Privacy Rule. A Covered Entity must make reasonable efforts to use, disclose and request only the minimum amount of Protected Health Information needed to accomplish the intended purpose of the use, disclosure or request.

Covered Entities are required to develop and implement the policies and procedures needed to reasonably limit uses and disclosures to the minimum necessary information for the purpose. For example: When the minimum necessary standard applies to a use or disclosure, a Covered Entity may not use, disclose or request the entire medical record for a particular purpose unless it can specifically justify the whole record as the amount of information necessary to accomplish the purpose.

This “minimum necessary” requirement is not imposed when patient information is disclosed or requested by another health care provider for treatment, when the disclosure is to the individual who is the subject of the information (or to their representative,) when the use or disclosure is made pursuant to an authorization, when the disclosure is made to HHS for complaint investigation, compliance review or enforcement, when the use or disclosure is required by law, or when use or disclosure is required for compliance with the HIPAA Transactions Rule or other HIPAA Administrative Simplification Rules.
15. Aren’t Covered Entities permitted to disclose PHI to contracted vendors?

HIPAA generally requires that Covered Entities and the vendors who receive PHI from them enter into contracts to ensure that the vendor will properly safeguard Protected Health Information.

This written contract – called a Business Associate Agreement under the Health Information Technology for Economic and Clinical Health Act – must set forth the permitted and required uses and disclosures of PHI by the vendor or Business Associate, require that the Business Associate not use or further disclose the information other than as required by the Business Associate Agreement or by law, and require the Business Associate to provide appropriate employee training and implement the safeguards necessary to prevent unauthorized use or disclosure of the information, including implementing requirements of the HIPAA Security Rule with regard to electronic PHI.

16. Which vendors are Business Associates?

There’s much confusion on this point, because every Covered Entity naturally seeks to “cover the bases.” Unfortunately, the statutory answer is less than clear. A Business Associate is a person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or in the process of providing services to, a Covered Entity.

More specifically, a member of a Covered Entity’s workforce is not a Business Associate, but a covered health care provider, health plan or health care clearinghouse can be a Business Associate of another Covered Entity.

Business Associate functions and activities enumerated in the HIPAA Security Rule include claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing. Many Covered Entities like to be on the safe side and require BAAs from anyone with whom they exchange PHI. The only organizations that seem to have difficulty with these blanket requirements are, in my experience, those that have no intention of instituting patient privacy safeguards or employee training to protect PHI. In that respect, the Covered Entity is probably better off finding a Business Associate who will perform the required function and has no problem with the information security aspects of the agreement.

17. Can a Covered Entity also be a Business Associate?

Yes ... and this single element of inclusiveness is very important because many Business Associates believe they can refuse to sign a BAA because they are already a Covered Entity. I’ll give you the exact citation in the hope that it serves you as well as it has served me: 45 CFR § 160.103 deals with defining Business Associates and clearly states that “a Covered Entity may be a Business Associate of another Covered Entity.”

18. What is a “hybrid entity” under HIPAA?

HIPAA defines a hybrid entity as one that uses or discloses PHI for only a portion of its business operations. If all of an entity’s functions are covered by the Security Rule, the entity cannot be considered a hybrid.

Hybrid entities are required to create adequate firewalls between their healthcare components and other components of the business or organization. Transfer of PHI held by the healthcare component to other components of the hybrid entity is still subject to the HIPAA Privacy Rule and is allowed only under the same circumstances as would make disclosure permissible for a separate entity.
19. **What is meant by the term, “patient consent?”**

The HIPAA Privacy Rule permits, but does not require, Covered Entities to voluntarily obtain patient consent for uses and disclosures of PHI for treatment, payment and healthcare operations. Covered Entities that choose to obtain patient consent have relative freedom to design a process for obtaining consent that best suits their needs.

20. **Isn’t consent the same as “patient authorization?”**

No. Patient authorization is at odds with patient consent in that it is required by the Privacy Rule for uses and disclosures of PHI not otherwise allowed by the rule. Where the Privacy Rule requires patient authorization, voluntary consent is not sufficient to permit a use of disclosure of PHI unless it also satisfies the requirements of a valid authorization.

An authorization is usually a detailed document that gives the Covered Entity permission to use PHI for specific purposes which typically are other than those sanctioned by the TPO standard or to disclose PHI to a third party specified by the patient.

A proper authorization specifies a number of elements, including a description of the PHI to be used and discussed, the person authorized to make the use or disclosure, the person to whom the Covered Entity may make the disclosure, an expiration date, and – in some cases – the purpose for which the PHI may be used or disclosed.

With some limited exceptions, Covered Entities may not condition patient treatment or coverage upon providing an authorization.

21. **What type of permission must be obtained before PHI can be disclosed?**

To lawfully disclose patient PHI outside of TPO, the Covered Entity will require an authorization form signed by the individual. This sort of permission is not needed in certain emergencies, or when PHI is required by law.

22. **What information must an authorization form include?**

The authorization form should include:

- A specific description of information to be used or disclosed
- The name and location of the Covered Entity receiving the information
- The name and specific identification of individual making the request
- An expiration date for the authorization
- A statement of individual’s right to revoke authorization
- A statement that information disclosed may be re-disclosed
- The individual’s signature and date

If the authorization form is signed by a representative of the patient, a brief description of the signatory’s authority is also required. For example, “Representative is patient’s Power of Attorney.”
23. So, what is the real difference between “patient consent” and “patient authorization?”

Under the HIPAA Privacy Rule, a Covered Entity can voluntarily obtain patient consent for uses and disclosures of PHI required for TPO. An authorization is required under the Privacy Rule for disclosures not otherwise allowed ... in other words, for most disclosures outside TPO. In most cases, consent cannot substitute for authorization.

24. What restrictions does the Privacy Rule place on the use of PHI for marketing purposes?

Covered Entities are only allowed to conduct limited marketing without first obtaining an individual’s authorization. All other types of marketing require patient authorization. Limited marketing activities include face-to-face communication between Covered Entity and individual and promotional gifts of nominal value.

If the marketing effort involves some type of renumeration to the Covered Entity from a third party, the patient authorization must state that renumeration is involved.

25. Are Covered Entities allowed to disclose PHI to friends and family members?

Yes, provided that the patient is present prior to a use or disclosure of the patient’s PHI and the Covered Entity:

- Obtains the individual’s agreement
- Provides the individual with an opportunity to object, or
- Can reasonably infer that the individual does not object

If the patient is not present, on the other hand, or does not have the opportunity to object owing to incapacitation or an emergency circumstance, the Covered Entity may use best professional judgment to determine whether the disclosure is in the best interest of the individual. In these situations, only the minimum relevant PHI may be disclosed.

26. When can a Covered Entity use and disclose PHI without written authorization?

The list of situations in which PHI disclosure is allowed without authorization is actually lengthier than you might imagine. Without allowing an individual to object, a Covered Entity may release PHI:

- If the disclosure is required by law
- For purposes of TPO
- For public health activities
- When the individual is a victim of abuse, neglect or domestic violence
- For purposes of health oversight
- For judicial and administrative proceedings
- For law enforcement purposes
- For uses and disclosures about decedents
• For organ, eye or tissue donation purposes
• For research purposes
• To avert a serious threat to public health and safety
• For specialized government functions
• For workers’ compensation

27. What PHI must be conveyed in response to subpoena?

The “minimum necessary” standard typically does not apply when the disclosure is required by law. However, the Covered Entity is allowed to disclose only the PHI that is relevant to the subpoena. For example, if the Covered Entity is responding to a court order, the only allowable disclosure is PHI specifically authorized by the court order.

28. Can PHI be released to health insurance companies?

Yes, provided that the disclosure is made for quality assurance and assessment purposes.

Remember that the HIPAA Privacy Rule allows Covered Entities to use and disclose PHI to facilitate healthcare operations. Quality assessment and improvement processes are a facet of healthcare operations.

29. Can PHI that has been de-identified be disclosed without authorization?

Yes, provided that the PHI cannot be used to identify the individual.

30. To de-identify PHI, what information must be removed?

All information that would lead to identification of the individual patient must be removed before PHI is considered de-identified. This information includes:

• Name
• Address information
• All elements of dates (except the year)
• Birthdate
• Date of admission
• Date of discharge
• Date of death
• Telephone number
• Fax number
• Email address
• Social Security Number
• Medical record numbers
• Health plan beneficiary number
• Account numbers
• License or certificate numbers
• Device identifiers
• Vehicle identifiers
• URLs associated with the individual
• IP address
• Biometric identifiers
• Facial photographs
• Any other unique identifying characteristic, code or number

31. Are Covered Entities required to verify the identity of anyone seeking to use PHI?
Yes. The Privacy Rule requires that the Covered Entity verify the identity and authority of any individual requesting PHI.

32. What is a Notice of Privacy Practices?
The Notice of Privacy Practices is a document the Covered Entity generates and provides to the patient upon patient request. The Notice of Privacy Practices contains a description of the types of uses and disclosures permitted under the TPO standard, as well as a description of other reasons the Covered Entity may use or disclose PHI without the authorization of the patient. The Notice of Privacy Practices also sets forth patient rights under HIPAA and provides a summary of disclosures that can be made only with the patient’s written authorization.

33. What else is included in the Notice of Privacy Practices?
The Notice of Privacy Practices also includes a summary of the Covered Entity’s responsibilities under HIPAA, information about the process for filing a complaint with the Covered Entity or the Secretary of the Department of Health and Human Services, the name and telephone number of a contact person (usually a Privacy Officer) who can provide additional information, and the effective date of the Notice.

34. Is a receipt required for patients who are offered a Notice of Privacy Practices?
If the Covered Entity has a direct treatment relationship with the patient, the Covered Entity must make a good faith effort to obtain a written acknowledgement from the patient attesting that the patient was offered a copy of the Notice of Privacy Practices. Should the patient refuse to sign an acknowledgment, the refusal should be noted.
Covered Entities without a direct treatment relationship are not required to obtain a written acknowledge-
ment that the patient has received a copy of their Notice of Privacy Practices.

35. **Must the Notice of Privacy Practices be posted in a specific location?**

Covered Entities are no longer required to post a copy of their Notice of Privacy Practices, though many
continue to do so out of an abundance of caution. If the Covered Entity maintains a website, the Notice of
Privacy Practices must be made available via the website.

36. **What should a Covered Entity do if a patient refuses to sign an acknowledgement that he or she has been offered a copy of the Notice of Privacy Practices?**

The patient’s chart should note the date on which the patient refused to sign an acknowledgement, along
with a reason for the patient’s refusal, if one is available.

37. **How long must Covered Entities keep copies of their Notice of Privacy Practices?**

Covered Entities must retain copies of past Notices of Privacy Practices for six years.

38. **Must Covered Entities redistribute their Notice of Privacy Practices after each update?**

No. However, the updated Notice must be made available upon request. Health plans are an exception;
they are required to redistribute their Notice of Privacy Practices each time they make a material change
in the document.

39. **Does the Notice of Privacy Practices need to be in the native language of the patient?**

HIPAA requires only that the Notice be written in plain language. Obviously, the definition of “plain lan-
guage” is open to interpretation.

The law does not specify that the Notice be written in the native language of the patient who receives it.
However, Covered Entities serving certain patient populations are encouraged to develop alternate Notic-
es of Privacy Practices that may communicate individual rights and the Covered Entity’s legal responsibil-
ities more clearly.

40. **Are Covered Entities bound by patient requests to restrict access to PHI?**

While a Covered Entity must allow a patient to request that the use and disclosure of the patient’s PHI be
restricted, the Covered Entity is not required to agree to the request. If the Covered Entity does agree to
the restriction, however, PHI may not be used or disclosed in any manner that would violate the restriction.

If the individual who made the request was in need of emergency treatment and the PHI was needed to
provide emergency care, the Covered Entity could disclosure patient information to the healthcare provid-
er offering emergency treatment to the individual.
41. Can patients request that PHI be communicated in a certain manner?

Covered Entities must permit patients to request – and must accommodate reasonable requests – to receive PHI by alternative means or at alternate locations.

Health plans must permit individuals to request – and must accommodate reasonable requests – to receive communication of PHI from the health plan by alternative means or at alternate locations if the individual states that disclosure might pose a danger to the individual.

42. Does HIPAA provide patients access to their PHI?

Yes, the law gives the patient the right to inspect and obtain a copy of their PHI.

43. Is the patient entitled to receive all information included in their health record?

No. In particular, patients are not entitled to access psychotherapy notes, information on criminal, civil or administrative actions or proceedings, or information that a qualified provider has determined might endanger the life of the individual if he or she is provided access to it.

44. Is there any limit on the number of times a patient may request access to PHI?

No. The law sets no limit on how often a patient may request access to his or her PHI. In theory, this lack of limitation can cause severe problems for any Covered Entity; in actual practice, it does not pose much of a challenge.

45. How quickly must Covered Entities respond to requests for access to PHI?

If the PHI is stored onsite, the Covered Entity must provide access within 30 days. If the PHI is stored offsite, the Covered Entity must provide access within 60 days. If the Covered Entity is unable to provide access within that timeframe, the response period may be extended by no more than 30 additional days.

46. Can the Covered Entity assess a fee for providing PHI?

Yes. However, the fee can include only the cost of copying, including supplies and labor for copying the information the individual requests, postage, when the patient has requested that the copy or summary be mailed, and time required to prepare any summary or explanation requested by the patient.

47. Are patients permitted to request that amendments be made to their PHI?

Yes. The patient may request that the Covered Entity amend or change PHI in a designated record set.
48. Should requests to amend PHI be made in writing?
The Covered Entity is entitled to request that the patient make an amendment request in writing. This practice provides a record of the request.

49. Is the Covered Entity required to make any amendments that are inaccurate?
Many practice managers believe they are required to make patient-requested amendments. Under the Privacy Rule, however, Covered Entities can deny a request to amend PHI if the Covered Entity determines that the PHI or record that is the subject of the amendment request was not created by the Covered Entity, is not a part of the designated record set, would not normally be available for review or inspection, or is fundamentally accurate and complete.

50. How quickly must Covered Entities respond to patient requests to amend PHI?
The Covered Entity must respond to amendment requests within 60 days. In extenuating circumstances, a 30-day extension is allowed.

51. Is the Covered Entity allowed to assess a fee for amending PHI?
No. No fee can be charged for amending PHI.

52. What is a Covered Entity required to do if a request to amend PHI is granted?
If the requested amendment is granted, the Covered Entity must notify the individual that the amendment was accepted.

Additionally, the Covered Entity should make an effort to obtain from the patient an authorization to inform relevant persons, and those persons should be specifically identified as part of the authorization.

The Covered Entity must then make an effort to provide the amended PHI to those persons identified by the individual requesting the amendment. This notification can include affected Business Associates.

53. What is a Covered Entity required to do if a request to amend PHI is denied?
If the patient’s request for amendment is denied, the Covered Entity must provide the individual with a “timely” written notice. This notice must explain the reason for the denial, the individual’s right to submit a written disagreement, the individual’s right to have the amendment request included in future disclosures, and the individual’s right to complain to the Covered Entity or to the Secretary of the Department of Health and Human Services.

If the individual submits a written disagreement, the Covered Entity may wish to create a written response or rebuttal. A copy of the response must be provided to the individual.

Future PHI disclosures must include the request for amendment or statement of disagreement, as well as the Covered Entity’s response or rebuttal. The Covered Entity is allowed to furnish a summary of the rebuttal in lieu of a full copy of the Covered Entity’s written response.
Section Three: Questions About PHI Disclosures

54. Can patients request PHI disclosure reports?
Yes. Under HIPAA, individuals have the right to receive an accounting of disclosures of their PHI made by a Covered Entity during the six years preceding the date on which the request is made. Note that there are some exceptions; the Covered Entity does not have to account for disclosures that meet the TPO Standard. Other exceptions include disclosures made:
  • To the individual
  • To people involved in caring for the individual
  • For national security and intelligence purposes
  • To correctional institutions or law enforcement personnel
  • In response to an authorization

55. How much time does a Covered Entity have to provide an accounting of PHI disclosures?
The Covered Entity must respond to a patient’s request for an accounting of PHI disclosures within 60 days. A 30-day extension is allowed for what the statute refers to as “extenuating circumstances.”

56. In an accounting of PHI disclosures, what must be included?
The Covered Entity must provide a written account of each specific disclosure, including the date the disclosure was made, the person to whom the information was disclosed, and a brief description of the disclosure.

The accounting process is easy enough when electronic PHI is at issue. I recommend that practices still using paper charts maintain a paper PHI Disclosure Accounting Log in each patient chart. Each disclosure is logged and a summary of disclosures can be made from the Log with a bare minimum of time expended to gather the information.

57. Is a Covered Entity allowed to charge a fee for providing an accounting of PHI disclosures?
A fee can be charged only when the individual requesting the accounting has requested another during the previous 12-month period. Otherwise, the Covered Entity is not allowed to charge for a disclosure accounting.

58. How is a “data breach” or unauthorized PHI disclosure actually defined?
The 2013 Interim Final Rule defined “breach” as the “unauthorized acquisition, access, use or disclosure of Protected Health Information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.”
The Interim Final Rule further provided that to be defined as a “breach,” the disclosure must pose a significant risk of financial, reputational or other harm to the individual. Other Federal agencies have similar standards for triggering a breach notification.

Section Four: Privacy Officers and Administrative Requirements

59. Who is responsible for implementing HIPAA procedures within a Covered Entity?

The law requires that all Covered Entities designate a privacy officer who is responsible for development and implementation of privacy policies and procedures. This individual also serves as a contact point, facilitates complaints and provides additional information about the Covered Entity’s privacy practices.

In my experience, only about two-thirds of Covered Entities have actually designated a privacy officer. Many of the privacy officers casually appointed by healthcare providers or administrators have no idea what their privacy officer responsibilities entail. For that reason, I highly recommend Smart Training LLC’s Privacy Officer training module.

60. Does a Privacy Officer need to be full-time or on the staff of the Covered Entity?

No, the Privacy Officer does not need to be full-time or on staff.

61. Is the Privacy Officer liable if the organization does not meet HIPAA requirements?

No. The Privacy Rule mandates that the owners or principles of a Covered Entity are liable for penalties arising from the actions of members of the workforce.

62. What are privacy policy and procedure training requirements?

The law requires that Covered Entities train staff members on privacy policies and procedures as required and necessary for members of the workforce to carry out their job functions.

63. Are Covered Entities required to provide privacy training to their Business Associates?

Only if a training requirement in the Business Associate Agreement specifically requires the Covered Entity to provide training. Otherwise, required training is the responsibility of the Business Associate.

64. What constitutes “certified” HIPAA training?

An example of “certified” HIPAA training would be an employee’s test scores achieved following completion of training. A good example of “certified” HIPAA training is the HIPAA course offered by Smart Training LLC. The program incorporates an exam after each section; as the participant moves through the content, he or she must correctly answer 75 percent of quiz questions in order to advance to the next section.
HIPAA standards require Covered Entities to document that their employees have received training. In the training industry, “certified” is taken to mean that there is some proof of performance relating to retention of training.

65. **What is the timeframe for providing privacy training to new workforce members?**

The Privacy Rule requires only that employees receive training “within a reasonable period” following employment. Some State laws – Texas, for example – stipulate that the training take place within a specific timeframe after hire. As amended, Texas House Bill 300 requires Covered Entities to train new staff members within 90 days of hire.

66. **How should a Covered Entity handle a complaint from a patient?**

The steps inherent in the complaint-handling process can vary from one Covered Entity to another. Complaints can generally be of three types: Complaints about policies and procedures, complaints about compliance with existing policies and procedures, or complaints about privacy requirements.

The law requires that every Covered Entity have a policy or procedure in place to document and resolve complaints. The details of the process are left to each Covered Entity to decide.

67. **How does a Covered Entity respond to lack of employee compliance with HIPAA?**

The Covered Entity must apply what the law refers to as “appropriate sanctions” against members of the workforce who demonstrate a lack of compliance with privacy policies and procedures. As with the procedure for handling complaints, development and implementation of “appropriate sanctions” is left to the Covered Entity.

68. **What if a Covered Entity discovers a Business Associate is not complying with HIPAA?**

If a Covered Entity becomes aware that a Business Associate is violating the Covered Entity’s privacy policies and procedures, the Covered Entity is required to “mitigate” the harmful effects of the actions of the Business Associate.

Ideally, the Business Associate can take immediate action to bring itself into compliance with the law. If this is not possible or if the Business Associate does not wish to take appropriate action, the Covered Entity should consider severing its relationship with the Business Associate.

The Covered Entity may then wish to report the Business Associate to the Department of Health and Human Services. Rather than a punitive measure toward the former Business Associate, this is a “cover yourself” action on the part of the Covered Entity.

69. **Can individuals waive the rights provided to them by HIPAA?**

No. Additionally, a Covered Entity may not require or otherwise try to induce an individual to waive his or her rights under prevailing HIPAA law.
70. What type of supporting documentation is required to show compliance by Covered Entities?

Ideally, a Covered Entity should maintain a compliance log. The log should contain procedural documentation needed to enforce the privacy policies set forth by the Covered Entity. Such a log might include an audit schedule, sample complaint resolution letters, a copy of the Covered Entity’s Notice of Privacy Practices, a copy of the Covered Entity’s Consent and Authorization forms, copying request approval and denial forms, PHI release forms, a plan for corrective actions when required, and employee and non-employee confidentiality agreements.

This is not an all-inclusive list, of course. The law requires records of policy and procedure development be kept for six years after the policy or procedure was instituted, amended, or discontinued.

71. When should a Covered Entity modify its HIPAA policies and procedures?

A Covered Entity is required to modify policies and procedures “as necessary and appropriate” to keep pace with changes in privacy law, or when the Covered Entity amends or alters a privacy practice.

72. What types of safeguards must Covered Entities have in place to protect PHI?

Covered Entities are required to have appropriate administrative safeguards, technical safeguards and physical safeguards in place to protect PHI from intentional and unintentional use or disclosure. While the requirements as set forth in the Privacy Rule are intentionally vague, they are more completely described in the HIPAA Security Rule.

The next several questions will focus on physical and technical safeguards. I’ll discuss administrative safeguards in the final section of this book.

Section Five: About Physical and Technical Safeguards

73. What are Physical safeguards?

Physical safeguards are the policies, procedures and other “physical measures” required to protect a Covered Entity’s electronic information systems, buildings and equipment from natural and environmental hazards, and unauthorized intrusion. Physical safeguards can include facility access controls, workstation use, workstation security, and device and media controls.

The Security Rule requires that Covered Entities implement physical safeguard standards for their electronic information systems, whether such systems are housed on the Covered Entity’s premises or another location.

74. What specific physical safeguards can ensure security of PHI?

Since physical safeguards for PHI refer to measures to protect the hardware and facilities that store PHI, the safeguards are directed at specific physical threats or vulnerabilities. These threats affect the security of PHI.
Some safeguards for electronic systems are similar to those used for securing paper-based systems, but some safeguards are obviously specific to healthcare IT. The policies and procedures that must be put in place to physically safeguard PHI include:

- Facility access controls – Physical access limitations bar unauthorized access to the areas where PHI is housed, while ensuring authorized personnel have unrestricted access.
- Workstation use – These specifications create the office policies for appropriate usage of workstations and the characteristics of the physical environment of workstations that access PHI.
- Workstation security – Incorporates restrictions on access to workstations mentioned above.
- Device and media controls – These constraints are designed to control the movement of hardware and electronic media that contain PHI into and out of the facility and the movement of these items within a Covered Entity, including disposal, reuse of media, accountability, and data backup and storage.

75. **What must Covered Entities do to ensure that media containing ePHI is properly stored?**

In all but the smallest offices, ePHI should be stored on a secure network server ... not on the hard drive of an individual workstation computer. More importantly, ePHI should not be stored on portable electronic media devices that can be easily removed from the Covered Entity's direct control.

Any ePHI stored on a portable device, such as a laptop, should always be encrypted, and such devices should never be left unattended.

76. **How can Covered Entities ensure that media containing ePHI is disposed of properly?**

Proper disposal methods include clearing (using software or hardware products to overwrite the media with non-sensitive data), purging (degassing or exposing the media to a strong magnetic field to disrupt the recorded magnetic domains), or physically destroying the media. Acceptable methods of physical destruction include disintegration, pulverization, melting, incinerating and shredding.

77. **What is described by the phrase “technical safeguards?”**

The technology involved in the use of ePHI – as well as policies and procedures that govern its use – are referred to as “technical safeguards.”

78. **Must data sent electronically or via email be encrypted?**

The use of encryption as a strategy for protecting in-transit ePHI is a technical and operational decision ... not something required by law. Covered Entities will typically conduct a risk analysis to determine whether encryption is necessary to protect ePHI during transmission.

79. **As part of their risk analysis, do Covered Entities need to examine network or individual computer activity?**

Yes. The Covered Entity is required to implement the software, hardware and procedural safeguards required to record and examine information system security on an ongoing basis.
80. Are technologies available to ensure the integrity of ePHI?

Yes. Several technologies are available; examples include checksum verification and error-correcting memory. All have one aim: To protect ePHI from improper alteration.

81. How does a Covered Entity guard against unauthorized access to ePHI that is being electronically transmitted?

Several other technical security strategies effectively guard against unauthorized access to ePHI being transmitted electronically.

To determine the technical security measures to implement, Covered Entities should review their current methods of transmitting ePHI. For instance: Is ePHI typically transmitted via email, over the Internet, or through some form of point-to-point or private network?

Once methods of transmission have been reviewed, the Covered Entity must identify the available and appropriate means to protect ePHI as it is being transmitted, select the appropriate solutions, and document the decision. The HIPAA Security Rule allows for ePHI to be sent over an “open” electronic network as long as that network is adequately protected.

Section Six: Strategies to Protect Electronic PHI

82. Why does the HIPAA Security Rule exist?

By now, you are familiar with the HIPAA Privacy Rule, which pertains to all forms of Protected Health Information and encompasses oral, paper and electronic transmission. The Security Rule, on the other hand, applies only to electronic Protected Health Information – ePHI.

There are three parts of the Security Rule with which Covered Entities and their Business Associates must comply: Administrative safeguards, Physical safeguards and Technical safeguards.

Each area within the HIPAA Security Rule offers implementation specifications – standard procedures for meeting the requirements in each area. Some implementation specifications are required, while others are “addressable.”

83. What information is protected by the HIPAA Security Rule?

The Security Rule is designed to protect four different types of data: Data in motion, which is data moving through a network, data at rest, which is data kept in databases and on servers, flash drives, etc., data in use, which is data in the process of being created, retrieved, updated or deleted, and data disposed of, which refers to data that has been discarded.

84. Are all Covered Entities affected by the HIPAA Security Rule?

Yes. All Covered Entities and Business Associates of Covered Entities must comply with Security Rule requirements.
85. **What is the object of the HIPAA Security Rule?**

The Security Rule works to ensure the confidentiality, integrity and availability of all ePHI created, received, maintained or transmitted by a Covered Entity or contracted Business Associate.

86. **How can a HIPAA Security Rule standard be “addressable?”**

“Addressable” means that the Covered Entity must implement the specification if it is reasonable and appropriate, but is not required to implement the specification if an alternative would accomplish the same purpose ... or if the standard may be met without implementing the specification or any alternative.

87. **Are administrative safeguards part of the Security Rule?**

Yes. Administrative safeguards encompass the administrative actions, procedures and policies that manage the development, implementation and maintenance of security measures designed to protect ePHI. The Administrative Safeguards portion of the Security Rule includes provisions for addressing operational and administrative security issues.

88. **What is meant by the term “security management” in the Security Rule?**

The Security Rule requires that Covered Entities implement specific policies and procedures designed to prevent, contain, detect and correct ePHI security violations.

89. **What is involved in performing a HIPAA risk analysis?**

While there are numerous methods of performing risk analysis, no single method or “best practice” guarantees compliance with the Security Rule.

Regardless of the method used, the Covered Entity’s Risk Analysis should detail the potential risks and vulnerabilities to the confidentiality, availability and integrity of all ePHI created, received, maintained or transmitted by the Covered Entity. The Risk Analysis should include ePHI in all forms of electronic media ... hard drives, CDs, media cards and portable devices.

Electronic media also incorporates single workstations and complex networks that may provide data to multiple locations. Consequently, a Covered Entity’s Risk Analysis should take into account all ePHI, regardless of the source or location, and irrespective of the particular electronic medium in which it is created, received, maintained or transmitted.

In the Risk Analysis, the Covered Entity should identify where ePHI is stored, received, maintained or transmitted, then identify and document all reasonably anticipated threats to that ePHI. Additionally, existing security measures should be assessed and documented. Are the measures required by the Security Rule already in place, and are current security measures properly configured and utilized?

The HIPAA Security Rule requires that Covered Entities take into account the probability of potential risks to ePHI. However difficult that process may sound, the results of this assessment, when combined with the initial list of threats, serves to determine which threats the Covered Entity is required to protect against because they are “reasonably anticipated.”
The Security Rule also requires consideration of the “criticality” or impact of the potential risk to the confidentiality, integrity and availability of ePHI. Risk levels are typically assigned for all threat and vulnerability combinations identified, and Risk Analysis documentation should detail assigned risk levels and list the corrective actions intended to mitigate each risk.

The Security Rule requires the Covered Entity’s Risk Analysis be documented, but it does not require that the documentation conform to any specific format. The analysis process should be ongoing and allow the Covered Entity to update and document security measures on an as-needed basis; continuous risk analysis allows the Covered Entity to identify when updates are required.

90. Who is responsible for implementing security requirements?
Covered Entities are required to name a Security Officer who is responsible for development and implementation of the policies and procedures required by the Security Rule. The Security Officer may be the Privacy Officer as well, but is more likely to be an IT specialist in a larger organization.

91. How is the decision made to allow or deny employee access to ePHI?
Access to ePHI must be assigned on a need-to-know basis. In other words, the decision to permit or deny access should be made on a case-by-case basis depending on the employee’s role in the organization.

Written policies should provide guidelines for supervision and authorization of employees who work directly with ePHI or who work in locations where ePHI can be accessed.

92. What about procedures that grant access to ePHI?
While this is more obvious to some Covered Entities than others, procedures should address the requirements for granting access to ePHI. Business practices and procedures governing access are among the essential requirements of the Security Rule.

93. If an employee is terminated, what can be done to maintain the security of the Covered Entity’s ePHI?
Termination procedures should include:
- Changing locks and lock combinations where necessary
- Timely removal from physical and logical access lists
- Removal of user account
- Deletion of personal files.

94. Are Covered Entities required to provide training to employees on the security of ePHI?
Yes. Covered Entities are required to provide specific training on security policies and procedures. This training should be offered to affected members of the workforce. The Security Rule also mandates that ePHI security training be updated periodically, but gives no guidance beyond that ambiguous requirement.
95. **Are Covered Entities required to monitor log-in access attempts?**

In most situations, yes. The Security Rule contains an “addressable” requirement regarding monitoring of user log-ins. A supervisor or administrator should monitor log-in attempts from unauthorized users through the audit and log files.

96. **What are Covered Entities required to do in the event of a security or data breach?**

I call this “the nightmare scenario,” but Covered Entities need to be prepared for the worst. This isn’t just my opinion; the Security Rule requires that the Covered Entity have a procedure in place to address and respond to known or suspected security incidents.

97. **What steps can Covered Entities take to plan for disasters and emergencies?**

Such contingency plans are not only recommended ... they are required by the Security Rule. Covered Entities must create and implement a contingency plan that incorporates procedures for continued operation in case of a natural or man-made disaster, emergency situation or unforeseen loss of data.

98. **What elements are usually included in a contingency plan?**

The HIPAA Security Rule outlines the elements of a contingency plan:

- Emergency response procedures to protect systems containing ePHI
- Data backup plan
- Disaster recovery plan
- Emergency operation plan.

99. **What is included in a typical data backup plan?**

The Covered Entity should have written procedures in place that create and continually maintain an “exact” copy (or clone) of ePHI. This means that the Covered Entity should have a backup procedure that effectively copies ePHI on all systems.

100. **What is a disaster recovery plan?**

A disaster recovery plan is designed and developed to create procedures that will restore lost ePHI. The disaster recovery plan should incorporate:

- Specifications for restoration of lost data
- Provision for recovering data to new systems in cases of system loss
- Provisions for all critical, server-based systems
- Provisions for periodic testing and review.
It’s hard to overstate the importance of a disaster recovery plan. Following Hurricane Sandy, for example, surveys of the 50,000 Covered Entities in Manhattan found that only half had working disaster recovery plans.

101. **How can Covered Entities ensure that their contingency plans will provide for a smooth transition during emergencies?**

Emergency conditions are notoriously difficult to create on demand. That fact may explain why the procedures for testing and revision of contingency plans are an addressable specification in the Security Rule.

Covered Entities are expected to use best judgment to determine the appropriate level and procedures for testing.

Most importantly, understand that every contingency plan is a work in progress. The Covered Entity is expected to continuously revise contingency plans to include significant changes in business operations and in the system or network environment.