The Definitive Guide to Complying with the HIPAA/HITECH Privacy and Security Rules

John J. Trinckes, Jr.
Chapter 3

Compliance Overview

Objectives
The objectives of this chapter are as follows:

- Understand that regulations are requirements that need to be met by the covered entity.
- Understand regulations assist in the development of policies.
- Understand procedures utilize standards to implement policies.
- Understand guidelines are set by procedures.
- Determine what is meant by reasonable safeguards to secure electronic protected health information.
- Determine what the covered entity should concentrate on in regard to becoming compliant.
- Understand the importance of conducting a risk assessment.
- Understand the importance of security awareness training.
- Determine if the covered entities’ current business associate agreements contain the required elements.
- Understand what will be expected from the audit pilot program designed by the Office for Civil Rights (OCR) to conduct compliance assessments on covered entities.
- Understand the differences between the SAS 70 and SSAE 16 audits.
3.1 Interrelationship among Regulations, Policies, Standards, Procedures, and Guidelines

There is sometimes a misconception that regulations, policies, procedures, standards, and guidelines are interchangeable or synonymous with one another. This could not be further from the truth. To understand their differences, these terms need to be fully defined as they relate to compliance. These terms will also be defined as it relates to the Health Insurance Portability and Accountability Act (HIPAA)/Health Information Technology for Economic and Clinical Health (HITECH) Act subject matter.

HIPAA/HITECH defines regulations that are mandated by law. These regulations must be implemented and compliance must be met, or there could be severe consequences. These regulations form the basis for the covered entities’ policies. Policies are the intentions of management to come into compliance with the regulations. Policies are high-level requirements that are documented and approved by management to direct employees in the process of complying with the stated objectives.

Standards are set by policies that help produce the procedures that will be followed to carry out the objectives of the policies. Standards attempt to tie the procedures with their policies. Procedures are more detailed than policies and normally provide step-by-step instructions to follow in complying with the policy. Normally, there is one policy statement and several procedures on what the covered entity should do to carry out the policy. Once the procedures have been developed, guidelines are usually established that further are common practices that are followed by employees of a covered entity and are normally the real-life practices that are in place as established by a given procedure. See Figure 3.1.

3.2 Reasonable Safeguards

As discussed earlier, a covered entity must have in place appropriate administrative, technical, and physical safeguards that protect against the unauthorized use or disclosure of protected health information. This does not mean that the covered entity’s safeguards will guarantee that such use or disclosure will not happen, but rather the potential risk of such activities is acceptable. Of course the safeguards implemented will vary from one covered entity to another based upon several factors, such as the covered entity’s size or nature of work. It is imperative that every covered entity conduct a risk assessment to determine what safeguards should be implemented based on their distinct requirements. A covered entity may be limited by resources, such as finances or administration; however, there are several examples of safeguards that do not require a lot of effort. Related to administrative controls, providing security awareness training to employees can provide a huge return by increasing the security posture of the covered entity. One technical control that is probably already in place is the use of passwords on
computer systems or programs that store protected health information. A physical control that could be implemented immediately is the practice of speaking quietly when discussing a patient’s condition or not using a patient’s name when walking through public areas.

### 3.3 Centers for Medicare and Medicaid Services Compliance Review

During 2009, five covered entities were reviewed for compliance with the Security Rule by the Office of E-Health Standards and Services (OESS) of the Centers for Medicare & Medicaid Services (CMS). Historically, these reviews were conducted after complaints were “filed against entities” (FAEs). However, covered entities were also reviewed during this year that had no complaints filed. The reason to take a little time to discuss the results of this review is that it gives the covered entity some insight as to areas of compliance that need improvements.
It appears that the following particular areas were focused on (Centers for Medicare & Medicaid Services [CMS] Office of E-Health Standards and Services [OESS] 2009):

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

Although the sample size for this review was rather small (only five individual covered entities were reviewed), CMS indicated the following areas of concern over all of them:

1. Risk analysis
2. Currency and adequacy of policies and procedures
3. Security training
4. Business associate agreements

Three other areas (workforce clearance, workstation security, and encryption) appeared to be issues from previous year (i.e., 2008) reviews, but CMS did not note these issues in the current review. Through the next several sections, areas of concern along with common pitfalls of the covered entities that CMS noted will be discussed.

### 3.3.1 Risk Analysis

The 2009 HIPAA Security Compliance Review indicated that covered entities are not performing the required risk assessments. The risk assessments are not reviewed on an annual basis or they were outdated based upon significant changes in the covered entities’ environment. It appears that the covered entities did not understand the process of conducting a risk assessment. The assessments reviewed were not formally documented or fully developed to cover all necessary steps in the risk assessment process. For instance, the risk assessments appeared to have skipped the first step in identifying systems that store, process, or transmit electronic protected
health information. These risk assessments failed to have a complete inventory of systems and locations where these systems are stored.

To mitigate these shortcomings, it is recommended that risk assessments be completed every 18 months or upon a significant change in the technical environment. A significant change in the environment can be brought on by introducing new systems such as electronic medical records solutions. Significantly upgrading existing systems or disposing of retired systems can alter the technical environment of the covered entity. Physically moving electronic assets to different locations can require additional physical controls be implemented. Any reorganization of the covered entity’s management or introducing new service offerings can require a change in the environment of the covered entity.

The risk assessments need to address all risks of the covered entity and establish an effective risk assessment process. This risk assessment process, described in detail in Chapter 12, includes identifying where data is stored and what systems are considered critical. Identifying threats and vulnerabilities to these systems along with analyzing the controls implemented to protect these systems can be determined by conducting vulnerability/penetration tests of these systems by experienced individuals. Exploiting these vulnerabilities will provide insight into the impact on the covered entity and assist in assessing the level of risks. By conducting these types of tests or exercises, the covered entity can determine additional controls that should be implemented. As previously discussed, the risk assessment should be formally documented and shared with executive level management to determine corrective actions for any deficiencies identified.

### 3.3.2 Currency and Adequacy of Policies and Procedures

According to the CMS, out of the five covered entities reviewed, only one had adequate policies and procedures implemented. Conditions of the review indicated that covered entities only had a few policies and procedures in place and most did not address the HIPAA/HITECH Security Standards and Implementation Specifications. In addition, actual guidelines followed were not consistent with the documented procedures or procedures did not follow the documented policies.

One of the recommended solutions is for covered entities to develop formally documented policies that are approved by management and reviewed on a periodic basis. In addition, the workforce member that is responsible for developing these policies and procedures must be one of the covered entity’s designated HIPAA security officers. The process for reviewing policies and procedures should include the following:

- Identify the management personnel responsible for the review
- The ability for workforce members to obtain the most recent version of the policies/procedures
Complying with the HIPAA/HITECH Privacy and Security Rules

Assess against current operational and regulatory requirements
Update as necessary
Document that the review was conducted
Communicate any updates to the other workforce members as necessary

Developing a standard policy and procedure format will enable consistency across relevant business units. To disseminate policies and procedures, the covered entity should look at a centrally managed repository solution that could automatically notify workforce members when updates occur. For example, this could be performed through an intranet site to inform workforce members of changes or through another type of shared portal that can notify workforce members of updates to policies and procedures. Posting changes in common areas could also provide notification to workforce members of updates. Security awareness training should reiterate any updates to policies and procedures and how these updates are made public to workforce members along with expectations of workforce members to keep abreast of these changes.

In regard to conducting periodic evaluations of policies and procedures, the individuals conducting these reviews should not be the same individuals responsible for the processes under review. These individuals should also have expertise or a reasonable level of competence when conducting these assessments. There are several methods that can be utilized to carry out these reviews such as walkthroughs of the process, interviews of workforce members, assessment of results, or actual testing of controls to determine effectiveness of the policy or procedure in place. For larger covered entities the internal audit team may be utilized to conduct the review as long as they have an appropriate level of separations of duties and competencies to conduct such audits. For smaller covered entities or in larger entities that may not have the expertise in-house, an independent third-party service provider should be contracted to assist the covered entity in determining their level of compliance.

3.3.3 Security Training

CMS determined that covered entities do not have policies and procedures in place to address the HIPAA/HITECH Security Rule provisions for security awareness training. For those covered entities that did have policies and procedures in place, they inadequately address the Security Rule requirements. When training was conducted, covered entities did not document or retain evidence of the training as required. In addition, security awareness training was not conducted prior to workforce members being granted access to systems containing electronic protected health information and refresher training was not provided on a regular basis.

Recommendations for these deficiencies are probably self-explanatory. However, as a point of reference, the covered entity needs to develop formal documented security awareness training policies that require new workforce members to receive training prior to gaining access to electronic protected health information. Security
Compliance Overview

Awareness training should be provided to all workforce members as a refresher on an annual basis and training material should be updated at least on an annual basis or when necessary. Furthermore, any identified threats through the risk assessment process should be incorporated into the security awareness training. One example of such risk that may be identified is that posed by workforce members working remotely to access electronic protected health information. Finally, attendance of security awareness training needs to be documented, retained, and there should be predetermined sanctions for any workforce member failing to complete this mandatory training or managers that fail to have their members provided with this training.

3.3.4 Business Associate Agreements

There appear to be many deficiencies noted by CMS when it comes to the agreements between business associates and the covered entity. First, the covered entities reviewed had business associates, but there were no business associate agreements (BAAs) between them. Second, there may have been a BAA, but it was not signed by both parties as required. Finally, the BAAs did not address certain requirements dictated by the regulation such as addressing the HIPAA/HITECH Security Rule, developing a comprehensive risk management program, reporting vulnerabilities, reporting breaches, performing activities, and the right of the covered entity to perform an audit on the business associate or require corrections to any deficiencies discovered during the assessment.

It is recommended that covered entities develop a comprehensive process to define the requirements and selection criteria for a business associate. A covered entity should focus on the business processes of the business associate and vet these categories accordingly. A covered entity should develop a standardized template and process of review to document the completion, date, and signatures of both the covered entity and business associate entering into the agreement. The review of the agreements should be conducted at least annually and the procedures should be standardized to document the preamble, body, terms/conditions, and penalties of all business associate agreements.

A contractual document should be developed to describe the business relationship, the services provided, the flow of HIPAA/HITECH Security Rule Standards and Implementation Specifications, and the flow of the specification for the Minimum Necessary Rule regarding electronic protected health information. The business associate contract should have:

- A start and end date
- Full service description
- Delivery terms/conditions
- Delivery specifications
- Requirements for conducting a periodic risk assessment and reporting results to the covered entity
3.4 HIPAA/HITECH Privacy and Security Audit Program

To ensure compliance with the HIPAA/HITECH Privacy Rule, Security Rule, and the Breach Notification Standards, the Department of Health and Human Services (HHS) is required under Section 13411 of the HITECH Act to conduct periodic audits of covered entities and business associates. The Office for Civil Rights (OCR) established a pilot program that would perform these mandated audits on up to 150 covered entities between November 2011 and December 2012. The program’s objectives are to identify compliance opportunities, best practices, and new risks or vulnerabilities that were not discovered through OCR’s complaint investigation and compliance reviews. This program is a new part of OCR’s overall health information privacy and security compliance program.

There were three steps in the process of this pilot audit program. First, starting around July 2011, there was the development of the audit protocol. Just as discussed earlier, this was the test plan development phase. To make sure the testing protocols will work, a small sample of about 20 audits would be conducted. Covered entities were selected, notified, and the audits were performed utilizing the developed testing protocols in phase 2. A review was conducted and changes were made, as necessary, to the testing protocols so that they could be implemented in a standardized manner to the rest of the covered entities chosen. Phase 3 would consist of completing the remaining audits by December 2012.

Of course, every covered entity and business associate could be eligible for an audit. In this first round of auditing, only covered entities such as health services, health plans, and healthcare clearinghouses were chosen. OCR is responsible for selecting the entities that would provide a broad and diverse assessment base. Related to the enforcement authority of the OCR, the covered entity should comply with the audit and cooperate fully with the auditor throughout this process. As of this writing, KPMG, LLP, was selected as the OCR auditor for this pilot program.

The audit will include a site visit along with an audit report. Utilizing an interview and observation process, the auditor will determine compliance with the privacy and security standards. The auditor will share the results with the covered entity allowing the covered entity to respond to any findings. A final report, with issues identified along with resolution actions of the covered entity, will be
submitted to OCR. The audit could take up to 30 business days to complete. Once the covered entity receives the notification letter that it was chosen for the audit, it has a limited number of days (i.e., 10 business days) to supply all requested documentation. This notification will commence between 30 and 90 days prior to the expected site visit. Onsite work could take between 3 and 10 business days with a draft of the audit report to follow around 20 business days thereafter. The covered entity will have an opportunity to respond to the findings within 10 business days and the final audit report will be submitted to OCR within 30 business days after the responses are received from the covered entity. These audits are primarily utilized for compliance improvement; however, serious violations could come under compliance review by OCR to address these issues.

The final audit report will include (Lamkin 2012):

- Covered entity’s name and description
- Methodology and timeframe
- Best practice observations
- Other related documentation such as data, interview notes, and checklists
- A listing of the following for each finding
  - Condition — The evidence to back up any notation of noncompliance
  - Criteria — Citation of the potential violation of the HIPAA/HITECH Privacy or Security Rule the finding presents
  - Cause — Supporting documentation to substantiate the reason a finding exists
  - Effect — The risk presented by the finding
  - Recommendations to mitigate the finding
  - Any corrective actions taken by the covered entity
- Conclusion
- Corrective action plan
- Recommendations to HHS (i.e., continued corrective action or future oversight recommendation)

3.5 SAS 70/SSAE 16 Debate

The American Institute of Certified Public Accountants (AICPA) developed the Statement on Auditing Standards number 70 (SAS 70) to focus on controls around internal financial reporting. Since data centers and colocations (COLOs) companies house systems that maintained financial reporting applications, users of these companies needed an objective opinion about these data centers. These users started to use the SAS 70 as a requirement before they would utilize the data center (or COLO) companies. The data center owners went out and conducted these audits, but it was not long before marketing got involved and claimed that their businesses were “SAS 70 certified” to validate their data centers. Unfortunately, the SAS 70 had no objective criteria. Some audit reports may have as little or as
many control objectives as the operators of the data center wanted to include on the report. In addition, these companies may claim to be audited even if they did not pass the audit. “The end result is that a SAS 70 audit means nothing without reading the details of the audit report” (Klein 2012). French Caldwell, research vice president at Gartner, concurs with this point by saying, “SAS 70 is basically an expensive auditing process to support compliance with financial reporting rules like the Sarbanes-Oxley Act (SOX). Chief Information Security Officers (CISOs), compliance and risk managers, vendor managers, procurement professionals, and others involved in the purchase or sale of IT services and software need to recognize that SAS 70 is not a security, continuity or privacy compliance standard” (Gartner 2010).

In an attempt to fix some of these issues with the SAS 70 audit, AICPA created a new standard known as the Statement on Standards for Attestation Engagements No. 16 (SSAE 16). The SSAE 16 now requires “the auditor to obtain a written assertion from management regarding the design and operating effectiveness of the controls being reviewed” (Klein 2012). The company can still choose its own controls, but as long as management attests to the fact that they follow these controls, they can claim to be SSAE 16 audited. It is still up to the report reader to decide the worth of the audit.

Since the SSAE 16 still focused on internal financial audits, the AICPA developed the Service Organization Controls 2 (SOC 2) audit specifically for data centers. To make things a little more confusing, however, they also developed the following (Klein 2012):

- Service Organization Controls 1 (SOC1) (also known as SSAE 16)—Type 1 and Type 2 that can be delivered from a SSAE 16 audit
- Service Organization Controls 2 (SOC 2)—Type 1 and Type 2 but can use up to five different control objectives as follows:
  - Security
  - Availability
  - Processing integrity
  - Confidentiality
  - Privacy of systems/information
- Service Organization Controls 3 (SOC 3)—Only audit that has a public seal that provides the same level of assurance as SOC 2 but does not provide a detailed description of tests performed. SOC 3 is intended for general release.

As a special note of reference, some companies are now claiming to be “SSAE 16 SOC 2 Certified”; however, there is no such certification available. “As long as users only look for the SSAE 16 audit checkbox, operators will be tempted to use the least rigorous audit criteria to simply pass the audit” (Klein 2012). This is synonymous with claiming to be “Certified HIPAA Compliant”; there is no such certification available as well. Per the HHS, “There is no standard or implementation
specification that requires a covered entity to ‘certify’ compliance” (Department of Health and Human Services Office for Civil Rights n.d.). Although 45 CFR § 164.308(a)(8) requires a covered entity to perform “a periodic technical and non-technical evaluation that establishes the extent to which an entity’s security policies and procedures meet the security requirements,” this evaluation can be performed by either internal or external organizations that provide evaluations or “certification” services. “It is important to note that HHS does not endorse or otherwise recognize private organizations’ ‘certifications’ regarding the Security Rule, and such certifications do not absolve covered entities of their legal obligations under the Security Rule” (Department of Health and Human Services Office for Civil Rights n.d.). Just because a covered entity conducted “certification” by an external organization does not mean that HHS will not subsequently find a security violation for which the covered entity will be held responsible.

As Caldwell states, “To ensure that vendor controls are effective for security, privacy compliance and vendor risk management, SAS 70, its successor Statements on Standards for Attestation Engagements (SSAE) 16, and other national audit standards equivalents should be supplemented with self-assessments and agreed-upon audit procedures” (Gartner 2010). Some of these other national audit standards include the following (Gartner 2010):

- Internal Organization for Standardization (ISO) standard certifications
- BITS Shared Assessments—Provided by a consortium of service providers, their customers, audit firms, and other third-party assessors
- SysTrust and WebTrust—Sponsored by AICPA and performed by qualified CPA auditors
- AT Section 101—Sponsored by AICPA and performed by qualified CPA auditors but a more flexible attestation procedure

3.6 Corporate Governance

Compliance along with information security is an enterprise-wide, corporate governance issue. Major decisions related to the way that compliance is handled in an organization need to be made at the highest level. With limits in budgets and resources, some covered entities have resorted to implementing a multitier approach to governance. This approach includes the following:

- An executive-level steering committee—Normally chaired by the chief information security officer. This committee is responsible for providing the overall broad strategy and commitment to information security efforts including compliance-related matters. This committee will establish budget limitations, goals, priorities, and actions that should be carried out by participants.
Advisory groups—These groups could be organized by projects or functions within the covered entity. These teams can provide detailed insights that can then be reported or recommended back to the steering committee.

Subcommittees—These subcommittees should include representation from across all areas of the covered entity.

Along with setting up an organizational structure, certain rules should be applied. For instance, certain proposals should come from certain responsible parties within the covered entity. These proposals require sponsorship from executive management and each one should have a business case to justify the need. Reviews should be conducted on the effect the proposals it may have on existing systems. Finally, the process developed needs to be adhered to and there should be no opportunity for bypassing by the decision makers.

The following are some additional rules that should be implemented to handle the corporate governance process (Morrissey 2012):

1. Chain the committees—The chairperson for one committee should be on the committee of the next upper level. For instance, the chairperson of one of the subcommittees should be on the executive-level committee that will make the decisions that the subcommittee is handling.

2. Set authority—Clear lines of authority should be drawn so that each committee is aware of the level of authority they have over certain decisions.

3. Make time worthwhile—Do not have meetings just to have them. For instance, if meetings are only providing status reports, e-mail these reports to responsible workforce members rather than having a meeting. Use meetings to make important decisions and discuss matters that could not be handled in other ways.

4. Use governance accordingly—Some covered entities are not at the level to implement this process. Know when the likelihood of success for such a method is appropriate.

5. Leaders should take a stand—Individuals in charge of the committees need to have the proper authority and can take a stand. If real change will take place, these leaders must be able to articulate their decisions and have the proper authority to carry them out.

3.7 Summary

This chapter explains the differences between regulations, policies, procedures, standards, and guidelines. A lot of individuals believe that these terms are interchangeable, but they have very different and specific meanings. An understanding of these differences is necessary to better comprehend the overall compliance process. Safeguards are the result of analyzing the necessary resources that must
be implemented to adequately satisfy compliance. These safeguards must be reasonably implemented based on several factors including financial, technical, and personnel resources available to the covered entity. Specific areas of concern were noted through the Centers for Medicare & Medicaid Services’ compliance review. These issues were published so that other covered entities can benefit from this insight to strengthen their own compliance efforts. As part of the HITECH enforcement requirements, the Office for Civil Rights hired KPMG, LLP, to conduct audits on 150 covered entities by the end of 2012. Although this audit is intended to assist in compliance efforts, severe violations may come under additional investigations. As discussed in Chapter 2, civil penalties can be severe and covered entities should take the appropriate actions to limit their risks of liability.

This chapter ended with a discussion on SAS 70 and SSAE 16 reporting. A lot of specific information was provided on the audits themselves, but one of the most important tips is that the reports, no matter what type, should be read and a determination should be made as to how well the organization under audit is conducting business.
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td>xxi</td>
</tr>
<tr>
<td>Preface</td>
<td>xxiii</td>
</tr>
<tr>
<td>Acknowledgments</td>
<td>xxvii</td>
</tr>
<tr>
<td>About the Author</td>
<td>xxix</td>
</tr>
<tr>
<td>Contributors</td>
<td>xxxi</td>
</tr>
<tr>
<td>Reviewer</td>
<td>xxxiii</td>
</tr>
<tr>
<td>Author’s Note</td>
<td>xxxv</td>
</tr>
<tr>
<td>Legal Disclaimer</td>
<td>xxxvii</td>
</tr>
<tr>
<td>HIPAA/HITECH Overview</td>
<td>1</td>
</tr>
<tr>
<td>Objectives</td>
<td>1</td>
</tr>
<tr>
<td>1.1 Definitions</td>
<td>4</td>
</tr>
<tr>
<td>1.2 Required by Law</td>
<td>7</td>
</tr>
<tr>
<td>1.3 Covered Entities Defined</td>
<td>8</td>
</tr>
<tr>
<td>1.4 Covered Transactions Defined</td>
<td>9</td>
</tr>
<tr>
<td>1.5 Are You a Covered Entity?</td>
<td>10</td>
</tr>
<tr>
<td>1.5.1 Covered Healthcare Provider</td>
<td>11</td>
</tr>
<tr>
<td>1.5.2 Healthcare Clearinghouse</td>
<td>13</td>
</tr>
<tr>
<td>1.5.3 Health Plan</td>
<td>14</td>
</tr>
<tr>
<td>1.5.4 Government Health Plans</td>
<td>15</td>
</tr>
<tr>
<td>1.6 Business Associates</td>
<td>17</td>
</tr>
<tr>
<td>1.6.1 Business Associate Contracts</td>
<td>17</td>
</tr>
<tr>
<td>1.7 Privacy Rule Overview</td>
<td>19</td>
</tr>
<tr>
<td>1.7.1 Permitted Use and Disclosures Overview</td>
<td>19</td>
</tr>
<tr>
<td>1.7.2 Authorized Uses and Disclosures Overview</td>
<td>20</td>
</tr>
<tr>
<td>1.7.3 Minimum Necessary Overview</td>
<td>20</td>
</tr>
<tr>
<td>1.7.4 Notice and Other Individual Rights Overview</td>
<td>20</td>
</tr>
<tr>
<td>1.7.5 Administrative Requirements Overview</td>
<td>21</td>
</tr>
<tr>
<td>1.7.6 Organizational Options Overview</td>
<td>21</td>
</tr>
</tbody>
</table>
1.7.7 Other Provisions: Personal Representatives and Minors
Overview ............................................................................22
1.7.8 State Law Overview..........................................................22
1.7.9 Enforcement and Penalties for Noncompliance
Overview ............................................................................22
1.7.10 Compliance Dates Overview............................................23
1.8 Electronic Transactions and Code Sets Rule Overview ..........23
1.9 National Provider Identifier Requirements Overview ..........24
1.10 Security Rule Overview...........................................................24
1.10.1 Administrative Safeguards Overview...............................25
1.10.2 Physical Safeguards Overview..........................................25
1.10.3 Technical Safeguards Overview.........................................26
1.10.4 National Institute of Standards and Technology
(NIST) Special Publications..................................................27
1.11 “Meaningful Use” Overview ..................................................27
1.12 Breach Notification Rule Overview.........................................29
1.13 Enforcement Rule Overview...................................................29
1.14 Anti-Kickback Statute ............................................................30
1.15 Patient Safety and Quality Improvement Act of 2005 (PSQIA) ......32
1.16 Consumer Privacy Bill of Rights .............................................32
1.17 Federal Rules of Civil Procedure ...........................................35
1.18 Summary ..............................................................................36
2 Relevance of HIPAA/HITECH to Healthcare Organizations.......39
Objectives ..............................................................................39
2.1 Why Is Security Important? ...................................................40
2.2 Are Healthcare Organizations Immune to Security Concerns? ......42
2.3 Suffering from Data Breaches ...............................................43
2.4 Rise of Medical Identity Theft ...............................................45
2.5 Internet Crimes Go Unpunished .............................................46
2.6 Social Engineering and HIPAA ..............................................47
2.6.1 Social Engineering: What Is It? ...........................................47
2.6.2 Tip 1: Learn to Identify Social Engineering Attacks ..............47
2.6.3 Tip 2: Security Awareness Should Be Personal and
Interactive .............................................................................48
2.6.4 Tip 3: Understand the Value of the Information They
Possess ..................................................................................48
2.6.5 Tip 4: Updates Are Essential ..............................................49
2.6.6 Tip 5: Develop Scripts .......................................................50
2.6.7 Tip 6: Have and Learn from Social Engineering
Assessments ...........................................................................51
2.6.8 Wrapping It Up ...............................................................51
2.7 Threats in the Workplace ......................................................51
3 Compliance Overview .................................................................. 61
   Objectives ................................................................................. 61
   3.1 Interrelationship among Regulations, Policies, Standards, Procedures, and Guidelines ................................................................................. 62
   3.2 Reasonable Safeguards .................................................................. 62
   3.3 Centers for Medicare and Medicaid Services Compliance Review ........................................................................................................ 63
      3.3.1 Risk Analysis ....................................................................... 64
      3.3.2 Currency and Adequacy of Policies and Procedures .................. 65
      3.3.3 Security Training ................................................................... 66
      3.3.4 Business Associate Agreements .................................................. 67
   3.4 HIPAA/HITECH Privacy and Security Audit Program ................ 68
   3.5 SAS 70/SSAE 16 Debate ................................................................. 69
   3.6 Corporate Governance .................................................................. 74
   3.7 Summary ................................................................................ 72

4 Privacy Rule Detailed .................................................................. 75
   Objectives ................................................................................ 75
   Background ................................................................................ 76
   4.1 Minimum Necessary .................................................................. 77
      4.1.1 Sample of Minimum Necessary Standard Policy ...................... 77
   4.2 Individual Consent ...................................................................... 79
   4.3 Permitted Uses and Disclosures Detailed ..................................... 79
      4.3.1 To the Individual .................................................................. 79
      4.3.2 Treatment, Payment, Healthcare Operations .......................... 79
      4.3.3 Uses and Disclosures with Opportunity to Agree or Object ......... 81
      4.3.4 Incidental Use and Disclosure ................................................... 82
      4.3.5 Public Interest and Benefit Activities ........................................... 82
      4.3.6 Limited Data Set ................................................................... 86
   4.4 Authorized Use and Disclosure .................................................. 87
      4.4.1 Valid Authorization Core Elements .......................................... 87
      4.4.2 Valid Authorization Required Statements .................................. 87
      4.4.3 Psychotherapy Notes ............................................................... 88
      4.4.4 Marketing .............................................................................. 88
4.5 Privacy Practices Notice ................................................................. 89
  4.5.1 Content of the Notice ............................................................ 90
    4.5.1.1 Sample of a Privacy Practice Notice ..................... 91
  4.5.2 Providing the Notice .......................................................... 94
  4.5.3 Acknowledgment of Notice Receipt .................................. 94
  4.5.4 Organizational Options ...................................................... 94
    4.5.4.1 Sample of Consent for Release of Protected Health Information .................. 94
    4.5.4.2 Sample of Revocation of Consent of Protected Health Information .......... 95
    4.5.4.3 Sample of Privacy Complaint Form ......................... 96
  4.5.5 Access .................................................................................. 96
    4.5.5.1 Sample of Request to Access Protected Health Information ................. 96
  4.5.6 Amendment .......................................................................... 97
    4.5.6.1 Sample of Request for Amendment of Protected Health Information ........ 97
  4.5.7 Disclosure Accounting ........................................................ 98
    4.5.7.1 Sample of Request for Accounting of Disclosures .................. 99
  4.5.8 Restriction Request ............................................................. 100
    4.5.8.1 Sample of Request for Restriction of Protected Health Information ........ 100
    4.5.8.2 Sample of Request for Restriction Termination 100
  4.5.9 Confidential Communications Requirements ....................... 101
    4.5.9.1 Request for Alternative Communications ................ 101
  4.6 Administrative Requirements .................................................. 102
    4.6.1 HIPAA Privacy Policies and Procedures .......................... 102
    4.6.2 Privacy Personnel ............................................................ 103
    4.6.3 Workforce Training and Management ............................ 103
    4.6.4 Mitigation .......................................................................... 104
    4.6.5 Data Safeguards ................................................................. 104
    4.6.6 Complaints ......................................................................... 104
    4.6.7 Retaliation and Waiver ....................................................... 105
    4.6.8 Documentation and Record Retention .............................. 105
    4.6.9 Fully Insured Group Health Plan Exception ...................... 105
  4.7 Organizational Options .............................................................. 106
    4.7.1 Hybrid Entity ...................................................................... 106
    4.7.2 Affiliated Covered Entity .................................................... 106
    4.7.3 Organized Healthcare Arrangement .................................. 107
    4.7.4 Covered Entities with Multiple Covered Functions .............. 107
    4.7.5 Group Health Plan Disclosures to Plan Sponsors ............ 107
  4.8 Other Provisions: Personal Representatives and Minors ............. 108
5 Electronic Transactions and Code Set Rule Detailed..................... 113
Objectives .................................................................................... 113
Background ................................................................................... 114
5.1 Definitions ............................................................................. 115
  5.1.1 ASC X12 Implementation Specifications ........................... 115
  5.1.2 Retail Pharmacy Specifications ......................................... 116
5.2 Standard Transactions ............................................................ 117
  5.2.1 Claims or Encounters ...................................................... 117
  5.2.2 Remittance Advice .......................................................... 118
  5.2.3 Eligibility Inquiry and Response ...................................... 118
  5.2.4 Prior Authorization and Referral ...................................... 118
  5.2.5 Claims Status Inquiry and Response .............................. 118
5.3 Medical Code Sets ................................................................. 118
  5.3.1 International Classification of Diseases (ICD) .................. 119
  5.3.2 National Drug Code (NDC) ............................................ 119
  5.3.3 Current Dental Terminology (CDT) ................................. 119
  5.3.4 Healthcare Common Procedural Coding System (HCPCS) and Current Procedural Terminology (CPT) ......................... 119
5.4 Local Codes ............................................................................ 119
5.5 Nonmedical Code Sets .......................................................... 120
  5.5.1 Provider Taxonomy Codes .............................................. 120
  5.5.2 Claim Adjustment Reason Codes .................................. 120
  5.5.3 Remittance Advice Remark Codes ............................... 120
  5.5.4 Claim Status Category Codes ........................................ 120
  5.5.5 Claim Status Codes ........................................................ 121
5.6 Requirements for Covered Entities ......................................... 121
5.7 Additional Requirements for Health Plans ............................... 121
5.8 Additional Rules for Healthcare Clearinghouses ...................... 122
5.9 Exceptions from Standards to Permit Testing of Proposed Modifications .......................................................... 122
5.10 Summary ............................................................................. 123

6 National Provider Identifier Requirements Detailed................ 125
Objectives .................................................................................... 125
Background ................................................................................... 126
6.1 Definitions ............................................................................. 126
6.2 Compliance Dates ................................................................. 126
6.3 Healthcare Provider’s Unique Health Identifier ............................. 126
6.4 National Provider System .............................................................. 126
6.5 Implementation Specifications for Healthcare Providers .............. 127
6.6 Implementation Specifications for Health Plans ............................. 127
6.7 Implementation Specifications for Healthcare Clearinghouses ....... 127
6.8 National Provider Identifier (NPI) Application ............................. 127
6.9 Summary ....................................................................................... 128

7 Meaningful Use Detailed .................................................................. 129
Objectives ................................................................................................ 129
Background ............................................................................................. 129
7.1 Meaningful Use Defined ................................................................. 130
7.2 Meaningful Use Criteria ................................................................. 130
7.3 Meaningful Use Requirements ....................................................... 130
7.4 Meaningful Use Stage 1 (2011 and 2012) ....................................... 131
7.5 Clinical Quality Measures ................................................................. 131
  7.5.1 Electronic Specifications ............................................................. 131
  7.5.2 Clinical Quality Measures for Eligible Professionals ............... 132
  7.5.3 Clinical Quality Measures for Eligible Hospitals and
      Critical Access Hospitals .............................................................. 132
  7.6 Alternative Reporting Mechanisms .............................................. 132
  7.6.1 Meaningful Use Core Measures for Eligible Professionals ....... 137
  7.6.2 Meaningful Use Menu Measures for Eligible Professionals .... 137
  7.6.3 Meaningful Use Core Measures for Eligible Hospitals
      and Critical Access Hospitals ...................................................... 140
  7.6.4 Meaningful Use Menu Measures for Eligible Hospitals
      and Critical Access Hospitals ...................................................... 142
7.7 Proposed Changes to Stage 1 and Proposals for Stage 2 .............. 144
7.8 Summary ....................................................................................... 146

8 Breach Notification Detailed ................................................................. 149
Objectives ................................................................................................ 149
Background ............................................................................................. 149
8.1 Definitions ..................................................................................... 151
8.2 Individual Notification .................................................................... 154
  8.2.1 Content of Notification ............................................................. 154
  8.2.2 Written or Electronic Notification ............................................ 154
8.3 Media Notification ........................................................................ 155
8.4 Secretary Notification ..................................................................... 155
  8.4.1 Sample Breach Notification Form ............................................ 156
8.5 Business Associate Notification ........................................... 157
8.6 Notification Delay Request of Law Enforcement ................. 157
8.7 Burden of Proof ................................................................... 158
8.8 Sample of Breach Notification Policy .................................. 158
8.9 Sample of Breach Notification to Individuals ...................... 159
8.10 Summary ........................................................................... 160

9 Enforcement Rule Detailed .................................................. 161
Objectives .............................................................................. 161
Background ............................................................................ 161
9.1 General Penalty .................................................................... 162
9.2 Affirmative Defenses ........................................................... 163
9.3 Waiver ................................................................................ 163
9.4 Notice of Proposed Determination ....................................... 163
9.5 Summary ........................................................................... 164

10 Security Rule Detailed .......................................................... 165
Objectives .............................................................................. 165
Background ............................................................................ 165
10.1 Implementation Specifications ............................................ 166
10.2 Implementation Process ..................................................... 166
10.3 Standards Are Flexible and Scalable ................................... 167
10.4 Security Standards Defined ................................................. 168
10.5 Policy and Procedure Drafting ............................................. 169
10.6 Documentation Requirements ............................................ 170
10.6.1 Time Limit—Required—45CFR § 164.316(b)(2)(i) .......... 171
10.6.2 Availability—Required—45 CFR § 164.316(b)(2)(ii) ...... 171
10.6.3 Updates—Required—45 CFR § 164.316(b)(2)(iii) ......... 172
10.7 Components of Policies ...................................................... 172
10.7.1 Sample of General Information Applicable to All ........ 173
Privacy and Security Policies.................................................. 173
10.8 Summary ........................................................................... 173

11 Security Rule: Administrative Safeguards .............................. 175
Objectives .............................................................................. 175
Background ............................................................................ 176
11.1 Security Management Process .......................................... 176
11.1.1 Risk Analysis—Required—45 CFR § 164.308(a)(1)(ii) .... 179
(A) ...................................................................................... 179
11.1.1.1 Sample of Risk Analysis Policy .............................. 182
11.1.2 Risk Management—Required—45 CFR §164.308(a) .... 182
  (1)(ii)(B) .......................................................................... 182
11.1.2.1 Sample of Risk Management Policy...................... 183
11.1.3 Sanction Policy—Required—45 CFR §164.308(a)(1)(ii)(C)................................................................................1
11.1.3.1 Sample of Sanction Policy....................................................184
11.1.4 Information System Activity Review—Required—45 CFR § 164.308(a)(1)(ii)(D).......................................................186
11.1.4.1 Sample of Information System Activity Review Policy ....................................................................................188
11.1.5 Assigned Security Responsibility—Required—45 CFR §164.308(a)(2).................................................................188
11.1.5.1 Sample of Designated Personnel Policy..........................190
11.2 Workforce Security..................................................................................191
11.2.1 Authorization and/or Supervision—Addressable—45 CFR § 164.308(a)(3)(ii)(A)...........................................................192
11.2.2 Workforce Clearance Procedure—Addressable—45 CFR § 164.308(a)(3)(ii)(B)...........................................................193
11.2.3 Termination Procedures—Addressable—45 CFR § 164.308(a)(3)(ii)(C).................................................................194
11.2.4 Sample of Workforce Security Policy.....................................195
11.3 Information Access Management..........................................................195
11.3.1 Isolating Healthcare Clearinghouse Functions—Required—45 CFR §164.308(a)(4)(ii)(A)....................................................196
11.3.2 Access Authorization—Addressable—45 CFR § 164.308(a)(4)(ii)(B).................................................................196
11.3.2.1 Sample of Access Authorization Policy .........................200
11.3.3 Access Establishment and Modification—Addressable—45 § CFR 164.308 (a)(4)(ii)(C).................................201
11.3.3.1 Sample of Access Establishment and Modification Policy.................................................................202
11.4 Security Awareness Training..............................................................202
11.4.1 Sample of Security Awareness Training Policy......................204
11.4.2 Security Reminders—Addressable—45 CFR § 164.308(a)(5)(ii)A).................................................................204
11.4.3 Protection from Malicious Software—Addressable—45 CFR § 164.308(a)(5)(ii)(B).................................................................205
11.4.4 Log-In Monitoring—Addressable—45 CFR § 164.308(a)(5)(ii)(C).................................................................207
11.4.5 Password Management—Addressable—45 CFR § 164.308(a)(5)(ii)(D).................................................................208
11.4.5.1 Sample of Password Policy..............................................209
11.5 Security Incident Procedures ................................................................209
11.5.1 Response and Reporting—Required—45 CFR § 164.308(a)(6)(ii)..................................................................................210
11.5.1.1 Sample of Security Incident Policy....................................213
11.6 Contingency Plan ........................................................................................................ 214
11.6.1 Data Backup Plan—Required—45 CFR § 164.308(a)(7)(ii)(A) ........................................... 215
11.6.2 Disaster Recovery Plan—Required—45 CFR § 164.308(a)(7)(ii)(B) ........................................ 218
11.6.3 Emergency Mode Operation Plan—Required—45 CFR § 164.308(a)(7)(ii)(C) ..................... 218
11.6.4 Testing and Revision Procedures—Addressable—45 CFR § 164.308(a)(7)(ii)(D) .................... 219
11.6.5 Applications and Data Criticality Analysis—Addressable—45 CFR § 164.308(a)(7)(ii)(E) ...... 220
11.7 Evaluation—Required—45 CFR § 164.308(a)(8) ................................................................. 220
11.7.1 Vulnerability/Penetration Testing ....................................................................................... 223
11.8 Business Associate Contracts and Other Arrangements ....................................................... 223
11.8.1 Written Contract or Other Arrangement—Required—45 CFR § 164.308(b)(4) .................... 226
11.9 Summary .............................................................................................................................. 226

12 Security Rule: Risk Assessments ...................................................................................... 229

Objectives .................................................................................................................................. 229
12.1 Risk Assessment Overview ................................................................................................. 229
12.2 System Characterization ..................................................................................................... 231
12.3 Threat Identification ............................................................................................................ 233
12.4 Vulnerability Identification .................................................................................................. 237
12.5 Control Analysis ................................................................................................................... 238
12.6 Likelihood Rating ................................................................................................................ 239
12.7 Impact Rating ....................................................................................................................... 240
12.8 Risk Determination .............................................................................................................. 241
12.9 Risk Mitigation .................................................................................................................... 242
12.10 Risk Management .............................................................................................................. 243
12.11 Risk Assessment Report .................................................................................................... 244
12.11.1 Administrative Controls ................................................................................................. 245
12.11.2 Physical Controls ............................................................................................................ 246
12.11.3 Technical Controls ......................................................................................................... 247
12.12 Summary .............................................................................................................................. 248

13 Security Rule: Security Awareness Training ...................................................................... 249

Objectives .................................................................................................................................. 249
Background ................................................................................................................................. 249
13.1 Training Strategy and Plan ................................................................................................. 250
13.2 Training Content, Materials, and Methods .......................................................................... 252
13.3 Implement Security Awareness Training ............................................................................. 253
13.4 Monitor and Evaluate Training Plan ................................................................................... 254
13.5 Sample Outline of Security Awareness Training ........................................ 254
13.6 Summary .................................................................................................. 260

14 Security Rule: Incident Response ................................................................. 261
Objectives ........................................................................................................ 261
Background ....................................................................................................... 261
14.1 Standard Format ........................................................................................ 262
14.2 Steps .......................................................................................................... 262
14.3 Notification ................................................................................................. 265
14.4 Incident Details .......................................................................................... 266
14.5 Incident Handler ......................................................................................... 267
14.6 Actions Taken or Recommended Actions ................................................... 267
14.7 Other Recommendations ........................................................................... 267
14.8 Summary .................................................................................................... 268

15 Security Rule: Business Continuity Planning and Disaster
Recovery ............................................................................................................. 271
Objectives ........................................................................................................ 271
Background ....................................................................................................... 272
15.1 Contingency Plan—45 CFR § 164.308(a)(7)(i) ........................................ 273
15.2 Data Backup Plan—45 CFR § 164.308(a)(7)(ii)(A) ................................... 274
15.3 Disaster Recovery Plan—45 CFR § 164.308(a)(7)(ii)(B) ............................. 275
15.4 Emergency Mode Operation Plan—45 CFR § 164.308(a)(7)(ii)(C) .......... 277
15.5 Testing and Revision Procedures—Addressable—45 CFR § 164.308(a)(7)(ii)(D)(b) ......................................................................................... 279
15.6 Applications and Data Criticality Analysis—Addressable—45 CFR § 164.308(a)(7)(ii)(E)(b) ............................................................................... 282
15.7 A Plan Addressing Both Operational and Regulatory Requirements ...... 284
15.8 Summary .................................................................................................... 296

16 Security Rule: Compliance Assessment ...................................................... 297
Objectives ........................................................................................................ 297
Background ....................................................................................................... 297
16.1 Gap Analysis .............................................................................................. 299
16.2 Develop or Modify Policies and Procedures .............................................. 300
16.3 Approve Policies and Procedures ................................................................. 300
16.4 Policy and Procedure Implementation ......................................................... 301
16.5 Test Plans ................................................................................................... 301
16.6 Assessment ................................................................................................. 302
16.6.1 Nontechnical Evaluation ..................................................................... 303
16.6.2 Technical Evaluation ........................................................................... 304
## 17 Security Rule: Physical Safeguards

<table>
<thead>
<tr>
<th>Subsection</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.1 Facility Access Controls</td>
<td>311</td>
</tr>
<tr>
<td>17.1.1 Contingency Operations—Addressable—45 CFR § 164.310(a)(2)(i)</td>
<td>313</td>
</tr>
<tr>
<td>17.1.3 Access Control and Validation Procedures—Addressable—45 CFR § 164.310(a)(2)(iii)</td>
<td>318</td>
</tr>
<tr>
<td>17.1.3.1 Sample of Access Controls Policy</td>
<td>319</td>
</tr>
<tr>
<td>17.1.3.2 Sample of Facsimile Machine Policy and Confidentiality Statement</td>
<td>319</td>
</tr>
<tr>
<td>17.1.3.3 Sample of E-Mail Policy and Confidentiality Notice</td>
<td>320</td>
</tr>
<tr>
<td>17.1.4 Maintenance Records—Addressable—45 CFR § 164.310(a)(2)(iv)</td>
<td>321</td>
</tr>
<tr>
<td>17.2 Workstation Use—Required—45 CFR § 164.310(b)</td>
<td>322</td>
</tr>
<tr>
<td>17.2.1 Sample of Log-On Warning Banner</td>
<td>324</td>
</tr>
<tr>
<td>17.2.2 Sample of Workstation Use and Location Policy</td>
<td>325</td>
</tr>
<tr>
<td>17.3 Workstation Security—Required—45 CFR § 164.310(c)</td>
<td>325</td>
</tr>
<tr>
<td>17.4 Device and Media Controls</td>
<td>328</td>
</tr>
<tr>
<td>17.4.1 Disposal—Required—45 CFR § 164.310(d)(2)(i)</td>
<td>329</td>
</tr>
<tr>
<td>17.4.2 Media Reuse—Required—45 CFR § 164.310(d)(2)(ii)</td>
<td>330</td>
</tr>
<tr>
<td>17.4.3 Accountability—Addressable—45 CFR § 164.310(d)(2)(iii)</td>
<td>330</td>
</tr>
<tr>
<td>17.4.4 Data Backup and Storage—Addressable—45 CFR § 164.310(d)(2)(iv)</td>
<td>331</td>
</tr>
<tr>
<td>17.5 Remote Use and Mobile Device Controls</td>
<td>332</td>
</tr>
<tr>
<td>17.5.1 Accessing Electronic Protected Health Information on Mobile Devices</td>
<td>332</td>
</tr>
<tr>
<td>17.5.2 Storing Electronic Protected Health Information on Mobile Devices</td>
<td>333</td>
</tr>
<tr>
<td>17.5.3 Transmitting Electronic Protected Health Information on Mobile Devices</td>
<td>334</td>
</tr>
<tr>
<td>17.5.4 Securing Wireless Networks</td>
<td>335</td>
</tr>
<tr>
<td>17.6 Summary</td>
<td>336</td>
</tr>
</tbody>
</table>

## 18 Security Rule: Technical Safeguards

<table>
<thead>
<tr>
<th>Subsection</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.1 Objectives</td>
<td>339</td>
</tr>
</tbody>
</table>
Contents

18. Background ...................................................................................... 340

18.1 Access Control ........................................................................... 340

18.1.1 Unique User Identification—Required—45 CFR § 164.312(a)(2)(i) ........................................................................ 344

18.1.2 Emergency Access Procedure—Required—45 CFR § 164.312(a)(2)(ii) ................................................................... 347

18.1.3 Automatic Logoff—Addressable—45 CFR § 164.312(a)(2)(iii) ........................................................................ 348

18.1.4 Encryption and Decryption—Addressable—45 CFR § 164.312(a)(2)(iv) .............................................................. 349

18.2 Audit Controls—Required—45 CFR § 164.312(b) ....................... 349

18.3 Integrity .......................................................................................... 351

18.3.1 Mechanism to Authenticate Electronic Protected Health Information—Addressable—45 CFR § 164.312(c)(2) ........................................................................ 353

18.4 Person or Entity Authentication—Required—45 CFR § 164.312(d) ........................................................................ 355

18.5 Transmission Security ..................................................................... 357

18.5.1 Integrity Controls—Addressable—45 CFR § 164.312(c)(2)(i) ........................................................................ 358

18.5.2 Encryption—Addressable—45 CFR § 164.312(c)(2)(ii) ..................................................................................... 359

18.6 Summary ....................................................................................... 359

19 Security Rule: Organizational Requirements .................................. 361

19.1 Business Associate Contracts—Required—45 CFR § 164.314(a)(2)(i) ........................................................................ 363

19.1.1 Sample Business Associate Contract ................................................. 365

19.2 Other Arrangements—Required—45 CFR § 164.314(a)(2)(ii) ...... 367

19.3 Requirements for Group Health Plans—Implementation Specifications—Required—45 CFR § 164.314(b)(2) .......... 368

19.4 Summary ....................................................................................... 369

20 Frequently Asked Questions .......................................................... 371

21 Checklists ........................................................................................ 389

21.1 Policies and Procedures .................................................................. 389

21.2 Document Request List ................................................................... 390

21.3 Incident Handling Checklist ............................................................. 391

21.4 Crisis Handling Steps ..................................................................... 392
The Definitive Guide to Complying with the HIPAA/HITECH Privacy and Security Rules
International Standard Book Number: 978-1-4665-0767-8 (Hardback)
© 2013 by Taylor & Francis Group, LLC
Foreword

The Health Insurance Portability and Accountability Act (HIPAA) was signed into law by President Clinton in 1996, and the son of HIPAA, the Health Information Technology for Economic and Clinical Health (HITECH) Act was signed into law in 2009 by President Obama as part of the American Recovery and Reinvestment Act.

One of the most often heard complaints about HIPAA is that it is far too broad, without adequate details and directives, which in turn leads to way too much interpretation in relation to HIPAA compliance.

That grievance seems to bear fruit in the fact that in 2011 half of the most significant data breaches involved stolen patient health data, according to a report by the consumer-advocacy group Privacy Rights Clearinghouse.

In The Definitive Guide to Complying with the HIPAA/HITECH Privacy and Security Rules, Jay Trinckes is providing a tremendous service to any HIPAA-covered entity in particularizing the gory technical details around HIPAA and HITECH that the U.S. Department of Health and Human Services never got around to documenting.

Why are medical systems such a target? For the attacker, a large metropolitan hospital billing system contains hundreds of thousands of credit card records in its database. It will have detailed medical information about politicians, entertainers, public officials, and more. It will have a storage area network (SAN) with perhaps a few terabytes of free space in which to store files, illegal content, and more.

Given that medical systems are such an enticing target, it is incumbent on the chief information officers and chief information security officers of those systems to ensure that they are adequately secured—and this book is a good place for them to start.

Ben Rothke, CISSP, CISM
The Department of Health and Human Services (HHS) has published four major rules implementing a number of provisions and regulations set out by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 1999 as part of the American Recovery and Reinvestment Act (ARRA). These rules are the Privacy Rule; the Electronic Transactions and Code Sets Rule; the National Identifier requirements for employers, providers, and health plans; and the Security Rule. It also includes more regulatory control over enforcement actions and stricter penalties for noncompliance. These rules apply to healthcare providers, healthcare clearinghouses, and health plans that are required to implement and comply with these rules, especially the Security Rule. Failure to implement or comply with these rules can leave the covered entity or others that need to comply open to large monetary fines, civil lawsuits, and other penalties.

With the rise of security breaches and other high-profile incidents regarding successful hacking events, it is very apparent that information has become a valuable commodity. The United States has transformed from a nation built on manufacturing and industry into an information/knowledge powerhouse. With the advancement in technology comes the opportunity for criminals to find another source of income by exploiting vulnerabilities within this technology. Retail, financial, and governmental entities have been the target and have fallen victim to these types of crimes; however, these industries are not the only industries susceptible. Technology has made companies more efficient and even now healthcare providers are required to submit Medicaid and Medicare reimbursement requests electronically. These capabilities have brought with them additional regulations for the healthcare industry. These regulations have brought to the forefront the importance of securing electronic protected health information (EPHI).

Just as a credit report is used to determine the credit worthiness for an individual, so will patient information eventually be used or already may be used to determine the health status of individuals. There has been a boom in the market of selling patient information to health and life insurance companies. These insurance
companies will rate individuals on their “health score” to determine their eligibility for a specific healthcare product or service.

Wherever there is money or financial gain to be made, there will be individuals who will attempt to get into the market. This can be done legally or illegally. Since the name of the game is information, the information becomes very valuable. This raises one major question: How well do you, as a healthcare provider, protect your clients’ medical records and patient information?

The Security Standards in HIPAA were developed to implement appropriate security safeguards for the protection of certain EPHI that may be at risk, while permitting authorized individuals to access and use this information under allowable uses.

Assessing these standards takes into consideration three fundamental security parameters: confidentiality, integrity, and availability (Figure 0.1).

This book was designed to assist the healthcare provider, or covered entity, in reviewing the accessibility of EPHI to verify that it is not altered or destroyed in an unauthorized manner and that it is available as needed by authorized individuals for authorized use. This book covers the following implementation standards and provides recommendations on how to comply with these standards, if required, to strengthen the security posture of the organization:

- Administrative safeguards
- Physical safeguards
- Technical safeguards
- Organizational requirements
- Policies/procedures and documentation requirements

Following the recommendations in this book will provide a covered entity the assurance that it is complying with the implementation standards of the Privacy...
and Security Rule of HIPAA/HITECH, along with providing recommendations based on other related regulations and industry best practices. This book can also help those entities that may not be covered but want to assure their customers that they are doing their due diligence to protect their personal and private information. Due to the fact that the HIPAA/HITECH rules apply to all covered entities and will most likely apply to business associates and subcontractors of business associates, it may not be long until these rules become the de facto standards for all companies to follow.

One of the most valuable parts of this book is the sample documents that are required and directions in using these policies/procedures to establish proof of compliance. This book will not take the place of a qualified individual conducting HIPAA assessments on the covered entity; however, the entity will be better prepared when the assessment is conducted or if an HHS auditor arrives at the door. The entity will also be well informed about taking the proper steps to protect its client’s information and strengthen its security posture. This can provide a strategic advantage to the organization, not only demonstrating to clients that it cares about their health and well-being but also cares about their privacy.
I would like to thank a number of individuals who assisted me in writing this book. First, I would like to thank my wife, Wendy. Without your support and encouragement, this book would have never been written. I will love you always and forever. Second, I thank my children, Traci and Brandon, for their understanding in allowing me to have the time needed to write.

I also thank my publisher, Richard O’Hanley, and all the members of CRC Press for their hard work. Your dedication to this project is unbeatable. I think we had some good success on our first book together and believe we have hit another home run with this one.

Finally, I thank all of my contributing authors and reviewers for their expertise and contributions.
John (Jay) Trinckes, Jr., CISSP, CISM, CRISC, CEH, NSA-IAM/IEM, MCSE-NT, A+, is the chief information security officer (CISO) for Path Forward IT, a managed service provider of IT and security services for the healthcare industry. Jay has previously worked as a senior information security consultant and authored The Executive MBA in Information Security, published by CRC Press, 2009. Trinckes has developed enterprise-level information security management programs for multiple clients along with conducting countless successful internal/external vulnerability/penetration assessments and other specific technical compliance audits. Trinckes has been instrumental in developing policies/procedures, audit plans, compliance assessments, business impact analysis, and business continuity and disaster recovery plans for several clients. He also conducts security awareness training and other presentations related to information security.

Trinckes is a Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC), and a Certified Ethical Hacker (C-EH). He holds certifications in the National Security Agency (NSA) INFOSEC Assessment Methodology (IAM) and INFOSEC Evaluation Methodology (IEM), along with Microsoft Certified Systems Engineer (MCSE-NT) and Comptia A+ Certifications. Trinckes provides a unique perspective on compliance as a result of his previous work experience as an information security risk analyst, IT manager, system administrator, and law enforcement officer.

Trinckes graduated with a bachelor’s degree in business administration/management information systems from the Union Institute and University with a 4.0 GPA and is currently working on multiple network- and security-related certifications. Trinckes is a member of numerous highly recognized security industry associations such as the FBI’s InfraGard®, Information Systems Audit and Controls Association (ISACA®), and the International Information Systems Security Certification Consortium (ISC²).

When Trinckes is not consulting or writing books, he likes to spend his spare time cooking, working out with his wife, and playing video games with his kids. Trinckes can be reached for assistance or comments related to this book at hitechpo@windstream.net.
The Definitive Guide to Complying with the HIPAA/HITECH Privacy and Security Rules
International Standard Book Number: 978-1-4665-0767-8 (Hardback)
© 2013 by Taylor & Francis Group, LLC
Contributors

Michael Stankiewicz. CISSP, CRISC, MBCI, is the vice president of security services for CastleGarde, Inc. He manages a team of six engineers to ensure CastleGarde’s 150-plus credit union clients are properly serviced. CastleGarde conducts internal and external vulnerability/penetration assessments, general IT controls assessments, online banking assessments, and specific technical compliance audits. In addition, Stankiewicz writes, updates, and performs independent analyses of business continuity plans and business continuity plan testing. He also conducts security awareness training and other presentations related to information security. Stankiewicz is a Certified Information Systems Security Professional (CISSP), Certified in Risk and Information Systems Control (CRISC), and a member of the Business Continuity Institute (MBCI). Prior to his time at CastleGarde, Stankiewicz’s notable work experience included time spent as the IT and forensic audit manager for the largest casino in the United States, vice president of information technology at a financial institution, security operations center engineer, and system administrator. He graduated with a bachelor’s degree in business administration from the University of Phoenix in Arizona. His personal interests include spending time with his wife and child, and extended family and friends, and participating in sports, including the historical re-enactment of baseball from the 1860s (http://vbba.org/), and home improvements. Stankiewicz can be contacted by e-mailing mike_stankiewicz@hotmail.com.

Chris Hadnagy (also known as loganWHD) is a professional social engineer who spends his time helping companies be secure and educated. He is a student of Paul Ekman’s training classes on micro expressions and has spent time learning and educating others on the values of nonverbal communication. He is also the lead developer of social-engineer.org as well as the author of the best-selling book Social Engineering: The Art of Human Hacking. He has launched a line of professional social engineering training and pen testing services at social-engineer.com. His goal is to help companies remain secure by educating them on the methods the “bad guys” use. Analyzing, studying, dissecting, then performing the very same attacks used by malicious hackers in some of the most recent attacks (i.e., Sony,
HB Gary, Lockheed Martin), Hadnagy is able to help companies stay informed and more secure. He runs one of the Web’s most successful security podcasts, The Social-Engineer.org Podcast, which spends time each month analyzing someone who has to use influence and persuasion in his or her daily life. By dissecting what he or she does, viewers can learn how to enhance their abilities. That same analysis runs over to the equally popular SEORG Newsletter. After two years, both of these have become a staple in most serious security practices and are used by Fortune 500 companies around the world to educate their staff. Hadnagy can be found online at www.social-engineer.com and on Twitter as @humanhacker.

**Ben Rothke**, CISSP, CISM (Twitter @benrothke), is an information security manager for a major hospitality firm and the author of *Computer Security: 20 Things Every Employee Should Know* (McGraw-Hill Professional Education, 2004).
Reviewer

Elizabeth Lamkin, MHA, is CEO of PACE Healthcare Consulting, LLC (www.pacehcc.com) in Hilton Head, South Carolina. After 20 years as a highly innovative hospital CEO, she now brings effective solutions to all types of hospitals and healthcare providers. Lamkin specializes in system development, quality, HIPAA, and billing compliance. Throughout her career, she has been repeatedly recognized for quality job performance as well as patient, staff, and physician satisfaction. She has extensive experience in both startups and turnarounds.

She is a nationally known speaker and author on billing compliance including CMS Recovery Audits.

Lamkin brings enterprise-wide solutions that begin with establishing clear directives for the governing board and creating strategic plans. Her techniques are based on performance improvement within a team of stakeholders, resulting in practical and sustainable solutions. These result-oriented techniques are relevant and transferable to any hospital or provider because each solution is based on the provider’s current systems and culture.

Lamkin received her bachelor of arts in interdisciplinary studies (BAIS), cum laude, from the University of South Carolina and a master’s in healthcare administration (MHA), also from University of South Carolina. She was named outstanding MHA student and won the Suzie James Yates scholarship.
Author’s Note

It has been my goal throughout this book to be as accurate in my writing as possible. I have attempted to explain the requirements of the HIPAA/HITECH regulations as clearly as possible and capture the intent of the requirements. In my research, I went to the official source of each regulation and if I thought the requirement was self-explanatory I cited it accordingly. In addition, if I believed any summation or paraphrasing of the requirement distorted the meaning, I cited the specific regulation in its entirety. It was not my intent to copy all of the regulations into this book since I trust that readers can look this information up for themselves; however, I would be remiss if I did not assist the reader by providing the detailed requirements as they are mandated in the regulations. To this end, it was my purpose to guide the reader through the intricacies of the HIPAA/HITECH regulations and to pave the way for an easier path to compliance. I hope that you will find that I have accomplished this goal.