FINAL HIPAA SECURITY REGULATIONS RELEASED – AT LAST

On February 20, 2003, the Department of Health and Human Services (HHS) published the Final Security Rule under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Final Security Rule or Rule).¹ It was in August of 1998 that HHS first published proposed regulations to implement information security requirements under the Administrative Simplification provisions of HIPAA (Proposed Security Rule). This Final Security Rule covers the administrative, technical and physical security measures that covered entities are required to take with regard to electronic storage and transmission of Protected Health Information (PHI). Because many of the security standards work in concert with the already finalized HIPAA Privacy Rule (Privacy Rule) that takes effect for most covered entities on April 14, 2003, health care providers have anxiously awaited the final version of these Rules.²

The Final Security Rule provides general principles and an implementation process, rather than detailed mandates or prescribed technologies. The Final Security Rule also allows covered entities to evaluate and determine how to apply many of the security standards based on the facts of each covered entity’s situation. The intent of the Rule is best summarized in the preamble where HHS stated, “we have focused more on what needs to be done and less on how it should be accomplished.”³

Most covered entities have until April 21, 2005, to comply with the Final Security Rule.¹

This advisory provides an overview of the Final Security Rule, details the types of transactions covered, specifies who must comply, and describes the administrative, physical and technical safeguards suggested to meet the security requirements. It also details a nine-point action plan for entities that must comply with the Final Security Rule by April 21, 2005, provides the security standard matrix from the Rule, and discusses how the issuance of this Rule will affect compliance with the HIPAA Privacy Rule, which goes into effect in just over a month—on April 14, 2003.

OVERVIEW OF THE FINAL SECURITY RULE

The Final Security Rule establishes guidelines for the minimum requirements to ensure confidentiality, security and integrity of electronically stored and transmitted health information. The Privacy Rule requires covered entities to implement “appropriate administrative, technical and physical safeguards” for PHI in all forms, including electronic and non-electronic. Covered entities have been waiting for the Final Security Rule to provide guidance on the meaning of the Privacy Rule’s “appropriate safeguards,” which are required under the Privacy Rule to be in place on April 14, 2003.⁵ The Final Security Rule does not provide specific instruction on how covered entities should safeguard PHI in oral, written or non-electronic form. However, it does provide a process of evaluation that covered entities could use to determine what would constitute “appropriate safeguards” under the Privacy Rule.

As noted, the overriding theme of the Final Security Rule is flexibility. The drafters stated that they wrote “the final rule to frame the standards in terms that are as generic as possible, and which, generally speaking, may be met through various approaches or technology.”⁶ The preamble states that each facility must analyze its own situation and work within the constraints of its situation and resources.

¹ The Federal Register lists the effective date for compliance with the regulations as April 21, 2005. 68 Fed. Reg. 8334. This stands in contrast to 45 C.F.R. § 164.318, which provides that April 20, 2005 is the compliance date for most covered entities. However, it is assumed that this is an oversight and will be corrected, since under the Congressional Review Act the Regulations cannot be effective for at least 60 days after publication – which would be April 21, 2003. Because the HIPAA statute provides for a two year period after “adoption” of the Rule before covered entities must comply, that makes the compliance date two years and 60 days after the date of publication in the Federal Register, or April 21, 2005 (assuming the Rule was sent to Congress prior to publication). Small health plans should have until April 21, 2006 to comply.

⁵ 45 C.F.R. § 164.530(c).

WHAT INFORMATION IS SUBJECT TO THE FINAL SECURITY RULE?

The Final Security Rule requires covered entities to safeguard and protect protected health information (PHI) maintained or transmitted in electronic form. Additionally, as part of the Final Security Rule, HHS updated the definition of PHI to clarify that PHI includes information that is transmitted by electronic media, maintained in electronic media or maintained in any other form or medium. The term “electronic media” is defined as: (1) electronic storage media including computer hard drives and any removable/transportable digital memory medium such as magnetic tape or disk, or digital memory card; (2) transmission media used to exchange information already in electronic storage media, for example extranet, leased lines, dial-up lines, private networks; and (3) the physical movement of removable/transportable electronic storage media. Further, the Final Security Rule clarifies that certain transmissions such as paper-to-paper faxes, person-to-person telephone calls, video teleconferencing and/or messages left on voice-mail are not “electronic media” and, accordingly, are not subject to the safeguards required under the Final Security Rule. Because HHS moved the definitions of electronic media and PHI to the general definition section in the HIPAA regulations, these definitions apply to all of the HIPAA Administrative Simplification regulations – i.e., security, transactions and code sets, and privacy regulations.

WHO MUST COMPLY WITH THE FINAL RULE?

The Final Security Rule provisions apply to three categories of entities. These three categories are the same as those under the Privacy Rule. Therefore, if an entity is a covered entity under the Privacy Rule, it is a covered entity under the Final Security Rule. The three categories of covered entities under the Final Security Rule are:

(1) Health plans;

(2) Health care clearinghouses; and

(3) Health care providers that transmit certain health claims transactions electronically.

---

7 C.F.R. §160.103.
8 Id.
10 C.F.R. §160.103.
Are Business Associates Subject to the Final Rule?

The Final Security Rule also mandates that covered entities must pass on information security requirements to their business associates.\(^\text{11}\) The good news is that the proposed requirement that there be so-called “trading partner agreements” with business partners who have access to electronic access to health information was not retained in the Final Security Rule. Instead, the Rule attempts to synchronize with the Privacy Rule by requiring that all business associate agreements provide that the business associate will: (1) implement administrative, physical and technical safeguards to protect electronic PHI it creates, receives, maintains or transmits on behalf of the covered entity; (2) ensure that any agent or subcontractor to whom it provides the covered entity’s electronic PHI agrees to implement safeguards to protect the PHI; (3) report to the covered entity any security incidents of which it becomes aware; and (4) authorize termination of the agreement by the covered entity, if the covered entity determines that the business associate has violated material terms of the agreement.\(^\text{12}\) As with the Privacy Rule, a covered entity generally will not be responsible for security breaches by its business associates unless it has knowledge of a breach and fails to take corrective action. These provisions reflect many of the business associate requirements under the Privacy Rule and likely will not necessitate major changes to existing business associate agreements. Nonetheless, as the April 2005 compliance date for the Final Security Rule approaches, covered entities should review their business associate agreements to ensure that they contain all of the required elements.

HOW IS THE FINAL SECURITY RULE STRUCTURED?

The Final Security Rule requirements are called “standards.” Each “standard” offers a generalized security requirement\(^\text{13}\) and is followed by an “implementation specification.” The “implementation specifications” identify what the covered entity must do to meet a standard\(^\text{14}\) and each one is either a “required specification” (R) or an “addressable specification” (A). The Final Security Rule contains both required and addressable implementation specifications and a security standards matrix (attached as an Appendix to this advisory) that designates the specifications with either an “R” or an “A.” A “required specification” must be implemented as stated in the regulation.

---

\(^\text{11}\) The term “Business Associate” is defined the same for the Privacy Rule as for the Final Security Rule. Essentially, it is a person to whom a covered entity provides PHI so that the person can provide a service to the covered entity. 45 C.F.R. § 160.103.

\(^\text{12}\) C.F.R. §164.314.

\(^\text{13}\) C.F.R. §160.103.

\(^\text{14}\) Id.
example, back-up data plans and disaster recovery plans are required specifications to the contingency plan "standard." 

For an "addressable specification" the covered entity is given more options. It must decide whether it will do one of the following: (1) address the specification directly; (2) implement an alternative that covers the same general concept identified in the standard; (3) do a combination of both; or (4) do nothing. The decision made by the covered entity must be based upon a security risk assessment and if the covered entity chooses to use an alternative solution, or decides to do nothing, the basis for that decision must be documented in writing. Included in the documentation should be the covered entity’s decision, the rationale behind the decision and an explanation of how the standard is being met. Cost can be used as a factor in these decisions, but the preamble to the Rule notes that adequate security measures still must be implemented, stating “[T]here is a clear requirement that adequate security measures be implemented . . . . Cost is not meant to free covered entities from this responsibility.”

**WHAT ARE THE PRIMARY COMPLIANCE OBLIGATIONS OF A COVERED ENTITY?**

The Final Security Rule specifies that covered entities must meet four general security requirements:

1. **Ensure the confidentiality, integrity and availability of all electronic PHI the covered entity creates, receives, maintains or transmits.**

2. **Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.**

3. **Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Final Security Rule.**

4. **Ensure compliance by the workforce.**

**HOW SHOULD THE BASIC SECURITY REQUIREMENTS BE MET?**

These requirements must be met by applying the standards found in the Final Security Rule. The security rule standards are grouped under three headings: administrative safeguards, physical safeguards and technical safeguards. The preamble explains

---


16 C.F.R. §164.306(d) and 68 Fed. Reg. 8369.


18 C.F.R. §164.306(a).

19 C.F.R. §164.306(c).
that: “The administrative, physical, and technical safeguards a Covered Entity employs must be reasonable and appropriate to accomplish the tasks outlined in paragraphs (1) through (4) above.”20 The covered entity will know what measures are reasonable and appropriate by engaging in a risk analysis and then implementing measures to handle the risks identified. Essentially, the covered entity must engage in a risk analysis to determine how to comply with the Security Standards. Compliance with the standards will be determined based on the effectiveness and feasibility of the measures in ensuring the confidentiality, integrity and availability of PHI.

**Administrative Safeguards**

The administrative safeguards are actions, policies and procedures to manage the selection, development, implementation and maintenance of security measures to protect electronic PHI and to manage the conduct of the covered entity’s workforce in relation to the protection of the information.21 Specifically, the administrative safeguards must address the following areas:

1. **Security Management Process:** Implement policies and procedures to prevent, detect, contain and correct security violations. There are four enumerated implementation specifications, all of which are required. These include: (a) a risk analysis to detect the potential risks and vulnerabilities; (b) risk management to implement security measures to reduce risks and vulnerabilities; (c) a sanction policy to apply appropriate sanctions against workforce members who fail to comply with the policies; and (d) information system activity review to review records of information system activity, such as audit logs, access reports and security incident tracking reports.22

2. **Assigning Security Responsibility:** Identify a security official to develop and implement policies and procedures.23

3. **Workforce Security:** Develop policies and procedures to ensure appropriate workforce access to electronic PHI and to prevent unauthorized access by those who should not have access to the information.24

---

21 C.F.R. §164.304.
22 C.F.R. §164.308(a)(1).
23 C.F.R. §164.308(a)(2).
24 C.F.R. §164.308(a)(3).
4. **Information Access Management:** Implement policies and procedures for authorizing access to electronic PHI. This includes isolating health care clearinghouse functions if they are part of a larger organization.\(^{25}\)

5. **Security Awareness and Training:** Implement a security awareness and training program for all members of the workforce (including management). The amount of training is to be determined by the facility.\(^{26}\)

6. **Security Incident Procedures:** Implement policies and procedures to address security incidents. This includes identifying and responding to suspected and known security incidents.\(^{27}\)

7. **Contingency Plan:** Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster) that damages systems containing electronic PHI. This requires developing and implementing a backup data plan, a disaster recovery plan and an emergency mode operation plan.\(^{28}\)

8. **Evaluation:** Perform a periodic technical and nontechnical evaluation, based initially on the standards, to see the extent to which the entity’s security policies and procedures meet the requirements of this section. The covered entity may make a business decision to obtain external certification, but is not required to do so to comply with the standard.\(^{29}\)

**Physical Safeguards**

Each covered entity is required to address the following physical safeguard standards that concern the physical protection of data systems and data from intrusion and from environmental or natural hazards.\(^{30}\) The physical safeguard standards are as follows:

1. **Facility Access Controls:** Implement policies and procedures to limit physical access to electronic information systems and the facilities in which they are housed, while ensuring that properly authorized access is allowed. These

\(^{25}\) C.F.R. §164.308(a)(4).

\(^{26}\) C.F.R. §164.308(a)(5).

\(^{27}\) C.F.R. §164.308(a)(6).

\(^{28}\) C.F.R. §164.308(a)(7).

\(^{29}\) C.F.R. §164.308(a)(8).

\(^{30}\) C.F.R. §164.304.
controls would include the following implementation features: disaster recovery, emergency mode operation, need-to-know procedures for personnel access and sign-in requirements for visitors.\(^{31}\)

2. **Workstation Use:** Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic PHI. For example, logging off before leaving a workstation unattended.\(^{32}\)

3. **Workstation Security:** Implement physical safeguards for all workstations that access electronic PHI, to restrict access to authorized users. A risk assessment will need to be performed to gauge the appropriate solutions to workstation security issues.\(^{33}\)

4. **Device and Media Controls:** Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic PHI into and out of a facility and the movement of these items within the facility.\(^{34}\)

The purpose of these standards is to protect a covered entity’s computer systems and related buildings and equipment from fire and other natural hazards, as well as unauthorized intrusion.

**TECHNICAL SAFEGUARDS**

The technical safeguard standards address the technology and the policies and procedures for its use that protect electronic PHI and control access to it.\(^{35}\) The following are included in the technical safeguards:

1. **Access Control:** Implement technical policies and procedures for electronic information systems (computers) that maintain electronic PHI to allow access only to those persons or software programs that have been granted access as specified by the security safeguards. This standard requires the assignment of a unique name and/or number for identifying and tracking user identity, and estab-

\(^{31}\) C.F.R. §164.310(a).

\(^{32}\) C.F.R. §164.310(b).

\(^{33}\) C.F.R. §164.310(c).

\(^{34}\) C.F.R. §164.310(d).

\(^{35}\) C.F.R. §164.304.
lishing procedures for obtaining necessary electronic PHI during an emergency. Some facilities may wish to use encryption as a method of denying access to information in a file.\textsuperscript{36}

2. **Audit Controls:** Implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI. These are to be put in place to record and examine system activity. Entities have flexibility in implementing the standard in a manner appropriate to their own needs.\textsuperscript{37}

3. **Integrity:** Implement policies and procedures to protect electronic PHI from improper alteration or destruction. Error-correcting memory and magnetic disc storage are examples of the built-in data authentication mechanism that are commonplace in hardware and operating systems today.\textsuperscript{38}

4. **Person or Entity Authentication:** Implement procedures to verify that a person or entity seeking access to electronic PHI is the one claimed. For example, digital signatures and soft tokens may be used to implement this standard.\textsuperscript{39}

5. **Transmission Security:** Implement technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network. Integrity controls and encryption are recommended to achieve this standard.\textsuperscript{40} It is interesting to note, however, that encryption is an \textit{addressable} specification and, therefore, is not specifically required to be implemented.

**OTHER NOTEWORTHY ITEMS**

**Documentation and Policy and Procedure Requirements**

The Final Security Rule requires covered entities to implement and maintain written policies and procedures to comply with the Final Security Rule. The same is true for any actions, activities or assessments required to be documented, such as the risk assessment analysis. Covered entities must maintain this documentation for six years from the later of the date of its creation or the date when it last was in effect.\textsuperscript{41}

\textsuperscript{36} C.F.R. §164.312(a).

\textsuperscript{37} C.F.R. §164.312(b).

\textsuperscript{38} C.F.R. §164.312(c).

\textsuperscript{39} C.F.R. §164.312(d).

\textsuperscript{40} C.F.R. §164.312(e).

\textsuperscript{41} C.F.R. §164.316.
HYBRID AND AFFILIATED ENTITY REQUIREMENTS

The Final Security Rule moves the provisions relating to affiliated covered entities and hybrid entities from the Privacy Rule to the general Administrative Simplification provisions and makes them applicable to both the Final Security Rule and the Privacy Rule. What this means is that the responsibilities of affiliated covered entities and hybrid entities for the maintenance of electronic PHI under the Security Rules can be implemented in the same manner as their responsibilities with respect to use and disclosure of PHI under the Privacy Rule.42

Sanctions for Noncompliance

Under the HIPAA statute, violations of the Final Security Rule can result in penalties of up to $100 per person per violation, up to a maximum of $25,000 for violations of a single standard during a calendar year.43 HIPAA statutory provisions also provide for criminal penalties for the knowing misuse of health identifiers or obtaining or misusing PHI of: (a) up to $50,000 and one year in prison for knowing violations; (b) up to $100,000 and up to five years in prison if the offense is committed under false pretenses; and (c) up to $250,000 and 10 years in prison if the offense is committed with “intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm.”44

No Safe Harbors

Not surprisingly, the Final Security Rule does not offer any safe harbor provisions. Therefore, it appears that the security measures adopted and utilized by covered entities will be judged after the fact, which will make the documentation and risk analysis process all the more important.

“De-identified” Information

Although not addressing the issue to any great degree, the preamble to the Final Security Rule notes that de-identified information is not covered by the Rule because it is no longer electronic PHI. However, any electronic PHI that is not de-identified must be used and secured in compliance with the Final Security Rule.45

---

42 C.F.R. §164.105.
43 P.L. 104-191, § 1176(1).
44 P.L. 104-191, § 1177(3).
AN ACTION PLAN FOR COVERED ENTITIES

Although April 21, 2005 is more than two years away, there are steps that should be taken now to ensure that your covered entity will be ready to comply with the Final Security Rule when compliance is required. Also, the general requirement under the Privacy Rule to implement “appropriate safeguards” for PHI takes effect on April 14, 2003. As a start, covered entities should begin to undertake the following nine-step action plan.

1. **Continue all measures necessary to be in compliance with the HIPAA Privacy Rule by the April 14, 2003 deadline.**

   The Final Security Rule does not extend the Privacy Rule compliance deadline of April 14, 2003. In terms of information security, the Privacy Rule requires that appropriate safeguards for PHI be in place by that date. At a minimum, these safeguards should include locking rooms and file cabinets where PHI is located, providing password protection for electronic files, and implementing policies on computer workstation use and the transmission of PHI by electronic means such as e-mail.

2. **Assemble an “information security team” and learn the security rules.**

   Covered entities should assemble an internal “information security team” and create a compliance agenda. The team should include members of a variety of hospital departments including the technology, information systems management, human resources, benefits, accounting, compliance and legal groups. The team should select an information security officer.

3. **Identify all electronic PHI maintained or transmitted by the covered entity.**

   The Final Security Rule applies to all electronic PHI, but not to written or oral forms of PHI. Therefore, covered entities should undertake a PHI mapping process to assess their use and transmission of electronic PHI in order to determine the information and data media that will fall under the requirements.

4. **Establish information access controls.**

   Covered entities should begin to draft written policies and procedures for electronic PHI access and controls. Among the procedures to be considered are implementation of unique log-in names, password protection of electronic files and means of tracking security incidents. In addition, covered entities should draft sanctions procedures for employees who violate the entity’s security policies, as well as personnel termination procedures to eliminate access to elec-
tronic PHI by former employees. For example, a checklist could be developed for employee termination that includes items such as changing locks, removing the employee’s passwords or other access to such information, removing user accounts and turning in keys or cards that allow access.

5. **Develop mechanisms to protect electronic PHI from improper use or destruction.**

Covered entities should begin implementing security mechanisms to verify that electronic PHI has not been altered or destroyed while being transmitted to or from the covered entity and implementing technical security measures to guard against unauthorized access to electronic PHI transmitted by the covered entity over an electronic communications network such as the Internet.

6. **Conduct risk analysis and implement risk management measures.**

The HIPAA security team should conduct a risk assessment identifying the potential risks of improper disclosure and vulnerability of electronic PHI maintained or transmitted in the covered entity’s database. This risk assessment should identify potential risks to the confidentiality of electronic PHI stored and transmitted by the covered entity or its business associates such as unauthorized access by former employees, hackers and the potentially devastating effects of computer viruses and worms. Covered entities must document their findings. After the security team conducts the assessment, it should develop and put in place a risk management program designed with sufficient measures to reduce the security risks and vulnerabilities identified in the risk assessment. It also should begin developing a contingency plan for responding to emergencies. This plan should list processes to create file backups, include a criticality analysis of what information is necessary to administer the covered entity, include a disaster recovery plan, and an emergency mode of operations plan, as well as testing and revision procedures.

7. **Begin security awareness and training.**

Similar to the Privacy Rule, the Final Security Rule requires each covered entity to train its workforce. Specifically, all employees with access to PHI, including management or supervisory employees, need to be trained on security provisions and the protection of electronic PHI. The training should involve awareness training, periodic security reminders, user education concerning virus protection or malicious software such as viruses and worms, emphasis on the importance of monitoring login success and failure and user education regarding passwords. The preamble to the Final Security Rule states that this training
could be provided as part of the new employee orientation with supplemental training as necessary, such as when new technologies are introduced or when changes are made to the security policy.

8. **Refer to NIST for risk assessment.**

On several occasions, HHS makes reference to guides published by the National Institute of Standards and Technology (NIST), as an aid in risk assessment and in the security management process. The NIST “800 Series” publications are important as practical guides that expand upon explanations by HHS of steps to follow and criteria to use, in assessing risk and managing security implementation. The guides also will be important references in enforcement of the security rules and in other litigation over security issues; therefore, a covered entity should consider consulting these guides as it works to address and implement the Final Security Rule.

9. **Ensure that business associate agreements include the Final Security Rule provisions.**

The Final Security Rule necessitates that business associate agreements include language protecting electronic PHI. As the security compliance date approaches, each covered entity should evaluate its business associate agreements to ensure that the language is broad enough to comply with both the Privacy and Final Security Rule provisions.

**CONCLUSION**

The Final Security Rule has been published and most covered entities have until April 21, 2005 to comply with the Rule. Just as important, however, covered entities should use the Final Security Rule as a guide to help implement compliance with the security provisions found in the HIPAA Privacy Rule with which they must be in compliance by April 14, 2003. The risk assessment and self-analysis provisions of the Final Security Rule can be used by covered entities in implementing the general security provisions contained in the Privacy Rule. Although the compliance date for the Final Security Rule may appear to be far off, covered entities should start working toward compliance now by setting up a security team and engaging in a thorough risk analysis to evaluate each of the security standards as applied to their entity. This analysis and the resulting decisions should be documented and appropriate protections should be implemented. April 21, 2005 will be here before we know it.

## Security Standards: Matrix

### Administrative Safeguards (see § 164.308)

<table>
<thead>
<tr>
<th>STANDARDS</th>
<th>SECTIONS</th>
<th>IMPLEMENTATION SPECIFICATIONS (R) = REQUIRED, (A) = ADDRESSABLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Management Process</td>
<td>164.308(a)(1)</td>
<td>Risk Analysis (R)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Risk Management (R)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sanction Policy (R)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Information System Activity Review (R)</td>
</tr>
<tr>
<td>Assigned Security Responsibility</td>
<td>164.308(a)(2)</td>
<td>Authorization and/or Supervision (A)</td>
</tr>
<tr>
<td>Workforce Security</td>
<td>164.308(a)(3)</td>
<td>Workforce Clearance Procedures (A)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Termination Procedures (A)</td>
</tr>
<tr>
<td>Information Access Management</td>
<td>164.308(a)(4)</td>
<td>Isolating Health care Clearinghouse Function (R)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Access Authorization (A)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Access Establishment and Modification (A)</td>
</tr>
<tr>
<td>Security Awareness and Training</td>
<td>164.308(a)(5)</td>
<td>Security Reminders (A)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Protection from Malicious Software (A)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Log-in Monitoring (A)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Password Management (A)</td>
</tr>
<tr>
<td>Security Incident Procedures</td>
<td>164.308(a)(6)</td>
<td>Response and Reporting (R)</td>
</tr>
<tr>
<td>Contingency Plan</td>
<td>164.308(a)(7)</td>
<td>Data Backup Plan (R)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Disaster Recovery Plan (R)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Emergency Mode Operation Plan (R)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Testing and Revision Procedure (A)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Applications and Data Criticality Analysis (A)</td>
</tr>
<tr>
<td>Evaluation</td>
<td>164.308(a)(8)</td>
<td>Written Contract or Other Arrangement (R)</td>
</tr>
<tr>
<td>Business Associate Contracts and Other Arrangements</td>
<td>164.308(b)(1)</td>
<td></td>
</tr>
</tbody>
</table>

### Physical Safeguards (see § 164.310)

<table>
<thead>
<tr>
<th>STANDARDS</th>
<th>SECTIONS</th>
<th>IMPLEMENTATION SPECIFICATIONS (R) = REQUIRED, (A) = ADDRESSABLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facility Access Control</td>
<td>164.310(a)(1)</td>
<td>Contingency Operations (A)</td>
</tr>
<tr>
<td>Workstation Use</td>
<td>164.310(b)</td>
<td>Facility Security Plan (A)</td>
</tr>
<tr>
<td>Workstation Security</td>
<td>164.310(c)</td>
<td>Access Control and Validation Procedures (A)</td>
</tr>
<tr>
<td>Device and Media Controls</td>
<td>164.310(d)(1)</td>
<td>Maintenance Records (A)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(R)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Disposal (R)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Media Re-use (R)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Accountability (A)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Backup and Storage (A)</td>
</tr>
</tbody>
</table>

### Technical Safeguards (see § 164.312)

<table>
<thead>
<tr>
<th>STANDARDS</th>
<th>SECTIONS</th>
<th>IMPLEMENTATION SPECIFICATIONS (R) = REQUIRED, (A) = ADDRESSABLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>164.312(a)(1)</td>
<td>Unique User Identification (R)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Emergency Access Procedure (R)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Automatic Logoff (A)</td>
</tr>
<tr>
<td>Audit Controls</td>
<td>164.312(b)</td>
<td>Encryption and Decryption (A)</td>
</tr>
<tr>
<td>Integrity</td>
<td>164.312(c)(1)</td>
<td>(R)</td>
</tr>
<tr>
<td>Person or Entity Authentication</td>
<td>164.312(d)</td>
<td>Mechanism to Authenticate Electronic Protected Health Information (A)</td>
</tr>
<tr>
<td>Transmission Security</td>
<td>164.312(e)(1)</td>
<td>(R)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Integrity Controls (A)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Encryption (A)</td>
</tr>
</tbody>
</table>
This Health Care Advisory is published by Alston & Bird to provide a summary of significant developments to our clients and friends. It is intended to be informational and does not constitute legal advice regarding any specific situation. This material may also be considered advertising under the applicable court rules. This advisory may be reprinted without the express permission of Alston & Bird so long as it is reprinted in its entirety including the Alston & Bird name and logo. If you have any questions or would like additional information, and/or if you would like to receive this information via e-mail, please contact your Alston & Bird attorney or the following:

Robert C. Lower  
404-881-7455  
rlower@alston.com

Betsy McCubrey  
(404) 881-4792  
bmccubrey@alston.com

Donna P. Bergeson  
404-881-7278  
dbergeson@alston.com

Angela T. Burnette  
404-881-7665  
aburnette@alston.com

Jennifer L. Butler  
202-756-3326  
jbutler@alston.com

Gina Hill Ginn  
404-881-4698  
gginn@alston.com

James A. Harvey  
404-881-7328  
jharvey@alston.com

John R. Hickman  
404-881-7885  
jhickman@alston.com

Gary E. McClanahan  
404-881-7632  
gmcclanahan@alston.com

Kim Ackourey Reddy  
404-881-7254  
kreddy@alston.com

Jack Spalding Schroder, Jr.  
404-881-7685  
jschroder@alston.com

Michelle A. Williams  
404-881-7594  
mawilliams@alston.com

If you would like to receive future Health Care Advisories electronically, please forward your contact information including e-mail address to healthcare.advisory@alston.com. Be sure to put “subscribe” in the subject line.

© Alston & Bird LLP 2003