

## **Final HIPAA Security Rule Allows Greater Flexibility**

**By: Andrew B. Wachler, Esq.**

**Abby Pendleton, Esq.**

**Amy Fehn, Esq.**

**Wachler & Associates, P.C.**

**210 East Third Street- Suite 204**

**Royal Oak, Mi 48067**

**(248) 544-0888**

**www.wachler.com**

On February 20, 2003, the Department of Health and Human Services (DHHS) published the long awaited Final Rule for the Health Insurance Portability and Accountability Act (HIPAA) Security Standards. This Final Security Rule addresses the integrity, confidentiality, and availability of protected health information that is maintained or transmitted electronically by those entities that have been designated as “covered entities” by HIPAA.<sup>1</sup>

HHS received approximately 2,350 comments to the proposed Security Rule that was published on August 12, 1998.<sup>2</sup> Many of these commenters objected to the failure of the government to adequately take into account the needs and capabilities of the various sizes and types of entities that are covered by the Security Rule. In the Final Security Rule, HHS attempted to incorporate the scalable and flexible approach that was adopted in the Final Privacy Rule, as well as to adopt terminology and standards consistent with the Privacy Rule.

The proposed Security Rule contained sixty-nine “implementation features” that were required for all entities. The Rule did not contain exceptions for small providers or providers who could achieve the same results in a different manner. The Final Security Rule takes such circumstances into consideration and changes many of the former “requirements” into “addressable” implementation specifications.<sup>3</sup>

The core structure of the Security Rule consists of eighteen standards, which are broken down into three basic categories: administrative safeguards, physical safeguards, and technical safeguards. Compliance with the standards is mandatory for all providers and there are thirteen implementation specifications associated with these standards that are also mandatory. It is the government’s position that these mandatory standards and required implementation specifications are “so basic, that no covered entity could effectively protect electronic protected health information without implementing them.”<sup>4</sup> The remaining implementation specifications are “addressable.”

---

<sup>1</sup> 68 Fed. Reg. 8334

<sup>2</sup> 68 Fed. Reg. 8335

<sup>3</sup> 68 Fed. Reg. 8336

<sup>4</sup> Id.

In determining whether or not to implement an “addressable” implementation specification, covered entities will be required to perform a risk analysis and explore available alternative options. Because health care attorneys are accustomed to advising clients with risk analysis in addressing compliance matters, they will play a vital role in this process.

Many software and hardware vendors have been marketing their wares to health care providers and other covered entities as being “required” by the HIPAA Security Rule. Due to the change in HHS’ approach in the Final Security Rule, covered entities should be encouraged to seek advice from legal counsel prior to making major technological purchases.

### ***Information Covered by the Final Security Rule***

The Security Rule protects the confidentiality, integrity, and availability of “electronic protected health information”. The definition of “electronic protected health information” includes “protected health information” as set forth in the Privacy Rule, to the extent that the information is maintained in an electronic medium.

Protected health information that is transmitted in an electronic medium also falls within the definition of electronic protected health information; however, HHS creates an exception for information that was not in electronic format prior to being transmitted. For example, information transmitted via facsimile or over a telephone system by voice or keypad is not considered to be electronic protected health information because it was not in electronic form before its transmission.<sup>5</sup> For the same reason, information stored on copy machines, videoconferencing systems, and voicemail are not considered electronic protected health information.<sup>6</sup>

As with the Privacy Rule, if information is de-identified, the Security Rule’s protections are no longer necessary.

A covered entity’s responsibilities under the Security Rule extend to all members of its workforce, including those who work at home.<sup>7</sup> For example, a provider office that allows its transcriptionist personnel to work at home must address the security requirements with regard to any electronic protected health information that is maintained, created or transmitted to or from the employee’s home.

Also note that the Final Security Rule covers electronic transmissions within a covered entity, as well as transmissions to outside entities.

---

<sup>5</sup> 68 Fed. Reg. 8342

<sup>6</sup> Id.

<sup>7</sup> 68 Fed. Reg. 8339

### ***Who Must Comply with the Final Security Rule?***

The Final Rule makes it clear that entities designated as “covered entities” under the Privacy Rule and the Electronic Standard Transaction Rule will also be required to comply with the Security Rule.<sup>8</sup>

As with the Privacy Rule, the Security Rule defines a “covered entity” as (1) a health plan; (2) a health care clearinghouse; or (3) a health care provider who transmits health information in electronic form in connection with one of the transactions designated by the Electronic Standard Transaction Rule.<sup>9</sup>

### ***General Overview of Requirements***

HHS sets forth certain general requirements of the Security Rule. It is the intent of HHS that all risk assessments and implementation decisions must take place with these requirements in mind.<sup>10</sup>

The general requirements closely mirror the language in the statute itself and require covered entities to do all of the following:

1. Ensure the confidentiality, integrity, and availability of all electronic protected health information 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 Subpart E of this part; and
4. Ensure compliance with this subpart by its workforce.<sup>11</sup>

HHS responded to several commenters regarding the use of the word “ensure” and acknowledged that it is impossible to ensure the absolute security of information. Although the language “ensure” is used in the HIPAA statute, HHS stated that “we note that the Congress also recognized that some trade-offs would be necessary, and that ensuring protection did not mean providing protection, no matter how expensive . . . . Therefore, when we state that a covered entity must ensure the safety of the information in its keeping, we intend that a covered entity take steps, to the best of its ability, to protect that information. This will involve establishing a balance between the information’s identifiable risks and vulnerabilities, and the cost of various protective measures, and will also be dependent upon the size, complexity, and capabilities of the covered entity . . . .”<sup>12</sup>

---

<sup>8</sup> 68 Fed. Reg. 8337

<sup>9</sup> 45 CFR §164.104

<sup>10</sup> 68 Fed. Reg. 8341

<sup>11</sup> 68 Fed. Reg. 8376

<sup>12</sup> 68 Fed. Reg. 8346

### ***Specific Standards and Implementation Specifications***

In order to meet the general requirements discussed above, HHS developed certain technology neutral standards that are broken down into the following three categories: administrative safeguards, physical safeguards, and technical safeguards. Notably, covered entities are mandated to meet the standards, but are given flexibility with regard to the specific technologies and measures that will be implemented.<sup>13</sup>

In determining which specific technologies and security measures must be taken in order to meet the standards, the covered entity is permitted to take the following into account:

1. Its size, complexity, and capabilities;
2. Its technical infrastructure, hardware, software, and existing security capabilities;
3. The costs of security measures; and
4. The probability and criticality of potential risks to electronic protected health information.<sup>14</sup>

While some standards are self explanatory, others include “implementation specifications” that serve as the “instructions” for implementing the standards.<sup>15</sup> These implementation specifications are divided into two categories: those that are “required” and those that are “addressable”.

### ***Required vs. Addressable Implementation Specifications***

If a specification is required, the covered entity must implement the specification as set forth in the Rule. For those specifications that are “addressable”, the covered entity may implement an alternative specification instead of, or in combination with, the specification set forth in the Rule. If an alternative approach is taken, the covered entity must document its decision not to implement the Security Rule’s specification, the rationale behind the decision, and the alternative approach that it has chosen.<sup>16</sup>

In some situations, the covered entity may also decide that the implementation specification is inapplicable to its situation and that the standard may be met without the specification or an alternative. In these situations, the covered entity must document its decision not to implement the specification, the rationale behind that decision, and the manner in which the standard is being met.<sup>17</sup>

The Final Rule also imposes a continuing obligation for covered entities to review the standards and implementation specifications as necessary to determine whether the

---

<sup>13</sup> 45 CFR §164.306(b)

<sup>14</sup> Id.

<sup>15</sup> 68 Fed. Reg. 8336

<sup>16</sup> 45 CFR §164.306(d)

<sup>17</sup> 68 Fed. Reg. 8336

specifications chosen continue to be reasonable and appropriate under the circumstances.<sup>18</sup>

### ***Administrative Safeguards: Standards and Implementation Specifications***

The administrative safeguards standards require covered entities to develop and maintain current documentation as appropriate to protect the health information in the covered entity's possession.

#### **1. Security Management Process Standard**

This standard requires covered entities to draft and implement policies and procedures designed to prevent, detect, contain, and correct security violations.<sup>19</sup> Many commenters requested removal of this standard because of the perceived burdens that it would impose on covered entities. However, the standard was maintained in the Final Rule because of HHS' position that this standard forms the foundation for the rest of the necessary security activities.<sup>20</sup>

With respect to this standard, HHS imposes four required implementation specifications: (1) risk analysis; (2) risk management; (3) sanction policy; and (4) information system review.

##### *a. Risk analysis*

The "risk analysis" implementation specification requires covered entities to identify the risks and vulnerabilities of the information in its care and take effective steps to minimize these risks and vulnerabilities.<sup>21</sup> In the comments to the Security Rule, HHS notes that covered entities should take into account all "relevant losses" that would be expected if security measures were not in place, including losses that would be caused by unauthorized uses and disclosures and loss of data integrity.<sup>22</sup>

##### *b. Risk management*

The "risk management" specification requires covered entities to take effective steps to minimize those risks and vulnerabilities discovered through the risk analysis process.<sup>23</sup> The goal of risk management should be to reduce risks and vulnerabilities to achieve the general requirements of the Security Rule discussed above.

---

<sup>18</sup> 45 CFR §164.306(e)

<sup>19</sup> 45 CFR §164.308(a)(1)(i)

<sup>20</sup> 68 Fed. Reg. 8346

<sup>21</sup> 45 CFR §164.308(a)(1)(ii)(A)

<sup>22</sup> 68 Fed. Reg. 8347

<sup>23</sup> 45 CFR §164.308(a)(1)(ii)(B)

c. *Sanction Policy*

Covered entities are also required to have sanction policies in place to appropriately discipline employees who fail to comply with the covered entity's security policies and procedures.<sup>24</sup> As in the Privacy Rule, the determination of specific sanctions is left to the discretion of the covered entity and should be based upon the covered entity's own human resource/employment policies, culture and the severity of the violation.<sup>25</sup>

d. *Information system activity review*

The final implementation specification that is required by the Security Management standard is the "information system activity review".<sup>26</sup> This requirement replaces the "internal audit" requirement in the proposed Rule. In making this replacement, HHS noted that the "internal audit" requirement had formal connotations that were not intended. The "information system activity review" implementation specification retains the internal review requirement, but gives covered entities flexibility to determine the extent, frequency, and nature of reviews.<sup>27</sup> Specifically, covered entities are required to "review records of information system activity such as audit logs, access reports, and security incident tracking reports."<sup>28</sup>

2. Assigned Security Responsibility Standard

This standard requires the covered entity to designate a "Security Official" and document this designation.<sup>29</sup> Much like the Privacy Official under the Privacy Rule, this individual will be responsible for development and implementation of the required security policies and procedures. Because this standard is self explanatory, there are no implementation specifications. While it may not be advisable for all covered entities, the Final Security Rule would allow covered entities to choose to designate a single individual as both the Privacy Official and the Security Official.<sup>30</sup>

3. Workforce Security Standard

This standard requires covered entities to implement policies and procedures to ensure that members of the workforce who need access to protected health information are given appropriate access.<sup>31</sup> The policies and procedures implemented by the covered entity must also ensure that those workforce members who do not need access are prevented from obtaining access. The implementation specifications under this standard are all addressable, rather than required. Because this Rule closely mirrors the Privacy Rule's

---

<sup>24</sup> 45 CFR §164.308(a)(1)(ii)(C)

<sup>25</sup> 68 Fed. Reg. 8347

<sup>26</sup> 45 CFR §164.308(a)(1)(ii)(D)

<sup>27</sup> 68 Fed. Reg. 8347

<sup>28</sup> 68 Fed. Reg. 8377; 45 CFR

<sup>29</sup> 45 CFR §164.308(a)(2); 68 Fed.Reg. 8347

<sup>30</sup> 68 Fed. Reg. 8347.

<sup>31</sup> 45 CFR §164.308(a)(3)(i)

minimum necessary requirements, covered entities are well advised to take minimum necessary policies into consideration when determining employees' access levels.

*a. Authorization and/or supervision*

The first addressable implementation specification under the “Workforce Security” standard is “authorization and/or supervision”.<sup>32</sup> In order to meet this specification, all employees who are not authorized to have access to protected health information would need to be supervised when working with electronic protected health information or when working in an area where the electronic protected health information is accessible. For example, maintenance and operations personnel may not be authorized to have access to electronic protected health information because it may not be necessary to perform their job. These individuals would need to be supervised while working with electronic protected health information.<sup>33</sup> The proposed Rule would have required “knowledgeable” personnel to supervise maintenance personnel at all times.<sup>34</sup> The Final Rule provides flexibility so that for example, operations and maintenance personnel must either be supervised or have authorization when working with electronic protected health information or in locations where it resides.

*b. Workforce clearance procedures*

The second addressable implementation specification is “workforce clearance procedures”. This implementation specification, if addressed, would involve the implementation of policies to determine whether a workforce member’s access is appropriate.<sup>35</sup> In responding to concerns generated by the proposed Rule, HHS specifically noted that “background checks” are not necessarily required by this specification.<sup>36</sup> The need for, and the stringency of, clearance procedures should be determined based upon the covered entity’s risk analysis. As an example of where this addressable specification may be determined to be unreasonable or inappropriate, HHS acknowledged that clearance procedures might be unnecessary in a small provider office where the only assistant is the provider’s spouse.<sup>37</sup>

*c. Termination procedures*

The third addressable implementation specification is “termination procedures”.<sup>38</sup> This specification addresses the implementation of procedures for terminating access to electronic protected health information with respect to a workforce member who is terminated or whose authorization to access electronic protected health information is terminated. The purpose of documenting termination procedures under this implementation specification is to ensure that termination procedures address security-

---

<sup>32</sup> 45 CFR §164.308(a)(3)(ii)(A)

<sup>33</sup> 68 Fed. Reg. 8348

<sup>34</sup> Id.

<sup>35</sup> 45 CFR §164.308(a)(3)(ii)(B)

<sup>36</sup> 68 Fed. Reg. 8348

<sup>37</sup> Id.

<sup>38</sup> 45 CFR §164.308(a)(3)(ii)(C)

unique actions to be followed. For example, the actions may be to revoke passwords and take back an employee's keys. Of particular benefit to small providers with limited resources, HHS removed all references to specific required activities that were contained in the proposed Rule, such as changing locks, noting that specific activities might not be reasonable for all covered entities.<sup>39</sup>

#### 4. Information Access Management Standard

The "Information Access Management" standard requires all covered entities to have policies and procedures in place setting forth how individuals will be authorized to access electronic protected health information.<sup>40</sup> The standard further requires that policies and procedures be consistent with applicable portions of the Privacy Rule, such as the Minimum Necessary requirements.<sup>41</sup>

This standard has one required implementation specification and two addressable implementation specifications as follows.<sup>42</sup>

##### *a. Isolating health care clearinghouse function*

The only required implementation specification applies only to those covered entities that include a clearinghouse as part of a larger organization. These covered entities must have policies and procedures in place to protect the electronic health information from being accessed by the larger organization.<sup>43</sup>

##### *b. Access Authorization*

The first addressable specification is "Access authorization" which involves the development and implementation of policies and procedures for granting access to electronic protected health information.<sup>44</sup> Examples include procedures for obtaining access through a workstation, a transaction, program, process or other mechanism.<sup>45</sup>

##### *c. Access Establishment and Modification*

The second addressable specification is "Access establishment and modification" which includes policies and procedures for establishing, documenting, reviewing, and modifying a user's right of access to a workstation, transaction, program, or process.<sup>46</sup>

In determining whether or not a covered entity will implement these addressable specifications, HHS notes that the determination will be based upon the size of the

---

<sup>39</sup> 68 Fed. Reg. 8349

<sup>40</sup> 45 CFR §164.308(a)(4)(i)

<sup>41</sup> 68 Fed. Reg. 8349

<sup>42</sup> 45 CFR 164.306(a)(4)(ii)

<sup>43</sup> 45 CFR §164.308(a)(4)(ii)(A)

<sup>44</sup> 45 CFR §164.308(a)(4)(ii)(B)

<sup>45</sup> 68 Fed. Reg. 8377

<sup>46</sup> 45 CFR §164.308(a)(4)(ii)(C)

covered entity and the degree of automation. HHS recognizes that it may not be necessary for a small provider to implement formal policies and could, instead, achieve the standard through a less formal process, such as a desktop standard operating procedure.<sup>47</sup> In addition, HHS acknowledges that this specification may be inapplicable to a small practice where all individuals have equal rights of access.<sup>48</sup>

## 5. Security Awareness and Training Standard

Covered entities are required to implement a security and training awareness program for all workforce members.<sup>49</sup> HHS specifically notes that security training is mandatory for all covered entities, regardless of size.<sup>50</sup> Because training may be tailored to the job needs of specific individuals, some members of the workforce may need only minimal training.<sup>51</sup> Four implementation specifications are associated with this standard, all of which are addressable, rather than required, thus, like the Privacy Rule, it gives covered entities considerable flexibility in determining how to conduct training programs. HHS does recommend a publication from the National Institute of Standards and Technology (NIST) as an “excellent source of information and guidance” on the subject of training programs.<sup>52</sup> In response to comments concerning training of business associates, HHS did note that covered entities are not required to provide training to business associates or others who are not part of their workforce.

### *a. Security Reminders*

The first addressable specification is the implementation of periodic security reminders or updates.<sup>53</sup> HHS notes in the preamble to the Final Rule, “training should be an ongoing, evolving process in response to environmental and operational changes affecting the security of electronic protected health information.”<sup>54</sup> Because of this expectation of HHS, covered entities with evolving technologies would be well advised to implement security updates even though the specification is technically addressable, rather than required.

### *b. Protection from malicious software*

The next addressable specification under the security and awareness training standard is “protection from malicious software”, including the implementation of procedures to detect, report, and guard against malicious software.<sup>55</sup> This specification replaces the “virus protection” implementation feature in the proposed Rule. The term “malicious

---

<sup>47</sup> 68 Fed. Reg. 8349

<sup>48</sup> 68 Fed. Reg. 8336

<sup>49</sup> 45 CFR §164.308(a)(5)(i)

<sup>50</sup> 68 Fed. Reg. 8350

<sup>51</sup> Id.

<sup>52</sup> Id. The specific publication referenced is NIST SP 800-16, “Information Technology Security Training Requirements, A role and performance base model”, April 1998.

<sup>53</sup> 45 CFR §164.308(a)(5)(ii)(A)

<sup>54</sup> 68 Fed. Reg. 8350

<sup>55</sup> 45 CFR §164.308(a)(5)(ii)(B)

software” was used instead of “virus protection” to include certain malicious software such as worms that are not technically considered viruses, but would still threaten the security, integrity, and availability of electronic protected health information.<sup>56</sup>

*c. Log-in Monitoring*

The third addressable specification under the security and awareness training standard is “Log-in monitoring”, including procedures for monitoring login attempts and reporting discrepancies.<sup>57</sup> For example, if a user gets an error message while trying to login, there is a risk that the user’s password is being used by an unauthorized person. Users would be instructed on when and how to report such discrepancies. Because the specification is addressable, a small entity could determine that this type of training was inapplicable, if, for example, there is only one computer terminal through which the information system could be accessed.

*d. Password management*

The fourth and final addressable specification under this standard is “password management” including procedures and training regarding the creation of passwords, how to change passwords, and how to safeguard passwords.<sup>58</sup>

**6. Security Incident Procedures Standard**

The security incident procedure standard requires covered entities to implement policies and procedures to address security incidents.<sup>59</sup> A security incident is defined in the Final Rule as “the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.”<sup>60</sup> This standard has only one required implementation specification.

*a. Response and reporting*

The requirements under the “Response and Reporting” implementation specification are similar to those imposed by the Privacy Rule with regard to privacy breaches. The specification requires covered entities to identify and respond to known security incidents, mitigate any harmful effects of the incident, and document security incidents and their outcomes.<sup>61</sup>

Like the Privacy Rule, covered entities are given discretion to determine exactly what information should be documented and the appropriate response.<sup>62</sup> In response to comments regarding external reporting of incidents, HHS noted that the Security Rule

---

<sup>56</sup> 68 Fed. Reg. 8349

<sup>57</sup> 45 CFR §164.308(a)(ii)(5)(c)

<sup>58</sup> 45 CFR §164.308(a)(5)(ii)(D)

<sup>59</sup> 45 CFR §164.308(a)(6)(i)

<sup>60</sup> 45 CFR §164.304

<sup>61</sup> 45 CFR §164.308(a)(6)(ii)

<sup>62</sup> 68 Fed. Reg. 8350

does not require any external reporting to outside entities and that such reporting would be up to a covered entity based on business and legal considerations.

## 7. Contingency Plan Standard

This standard requires covered entities to develop policies and procedures setting forth the way in which the covered entity will respond to emergencies or occurrences that could damage systems containing electronic protected health information. Examples of situations that the covered entity must plan for include fire, vandalism, system failure, and natural disasters.<sup>63</sup> With respect to natural disasters, each covered entity needs to consider its risk of being affected by various natural disasters and develop policies and procedures accordingly. HHS suggests in the preamble that if the risk of a natural disaster were low, the covered entity would not need to address it.<sup>64</sup>

HHS contemplates that contingency plans will vary significantly among covered entities and will range from highly complex processes to simple manual processes.<sup>65</sup>

The contingency plan standard has three required implementation specifications and two addressable specifications.

### *a. Data backup plan and disaster recovery plan*

The first two required implementation specifications are the “Data backup plan” and the “Disaster recovery plan.” These specifications require covered entities to develop policies and procedures for the creation and maintenance of a duplicate copy of all electronic protected health information that can be retrieved by the covered entity when necessary to restore any lost data.<sup>66</sup> Covered entities may choose to use paper copies of information as the backup and recovery.<sup>67</sup>

### *b. Emergency mode operation plan*

The third required implementation specification is “Emergency mode operation plan”, which is the development of procedures designed to enable the continuation of critical business processes allowing for the continued protection of the security of electronic protected health information during and immediately after a crisis situation.<sup>68</sup> As part of this plan, the covered entity should define exactly what information is needed to continue

---

<sup>63</sup> 45 CFR §164.308(a)(7)(i)

<sup>64</sup> 68 Fed. Reg. 8351. Specifically, in response to comments that the implementation of measures against a natural disaster would be too big an issue to address, HHS states that “The final rule calls for covered entities to consider how natural disasters could damage systems that contain electronic protected health information and develop policies and procedures for responding to such situations. We consider this to be a reasonable precautionary step to take since in many cases the risk would be deemed to be low.”

<sup>65</sup> 68 Fed. Reg. 8351

<sup>66</sup> 45 CFR §164.308 (a)(7)(ii)(A), (B)

<sup>67</sup> 68 Fed. Reg. 8336

<sup>68</sup> 45 CFR §164.308 (a)(7)(ii)(C); 68 Fed. Reg. 8351

to do business. For example, the covered entity must make decisions as to whether or not it is necessary to back up entire e-mail systems, or just e-mail for key individuals.<sup>69</sup>

*c. Testing and revision procedures*

“Testing and revision procedures” is an addressable implementation specification, which, if addressed, would involve the development and implementation of policies and procedures for testing backup and disaster recovery plans and revising these plans as necessary.<sup>70</sup> Although testing was required in the proposed Rule, HHS has since determined that testing and revision of all parts of a contingency plan might not be reasonable. In the preamble to the Final Rule, HHS discusses that a covered entity may consider factors such as its size, configuration, and environment when determining whether testing and revision of the entire contingency plan is reasonable.<sup>71</sup>

*d. Applications and data criticality analysis*

The final addressable implementation specification is “Applications and data criticality analysis”. This specification involves the assessment of a covered entity’s data and applications to determine which would be considered “critical” when developing data backup and disaster recovery plans.<sup>72</sup> As with the testing and revision specification discussed above, HHS determined that this requirement might not be reasonable for certain covered entities, depending upon their size, configuration, and environment.<sup>73</sup>

8. Evaluation standard

The “Evaluation” standard replaces the “certification” requirement that was contained in the proposed Rule. This standard requires covered entities to periodically perform an evaluation of both technical and non-technical security safeguards to determine whether the covered entity is in compliance with the Security Rule. Periodic evaluations must be performed any time there are environmental or operational changes that could affect the security of protected health information.<sup>74</sup>

In response to comments concerning whether the evaluation should be done by an external party, HHS clarifies in the preamble that the method of evaluation will be a business decision left to each covered entity and may be performed internally or externally. HHS further recognizes that external evaluations may be too costly for small entities.<sup>75</sup> Although HHS intends to develop technical assistance materials, these materials will not address various business environments. Note, however, that

---

<sup>69</sup> 68 Fed. Reg. 8354

<sup>70</sup> 45 CFR §164.308(a)(7)(ii)(D)

<sup>71</sup> 68 Fed. Reg. 8351

<sup>72</sup> 45 CFR §164.308 (a)(7)(ii)(E)

<sup>73</sup> 68 Fed. Reg. 8351

<sup>74</sup> 45 CFR §164.308(a)(8)

<sup>75</sup> 68 Fed. Reg. 8351

professional associations have been encouraged to assist with the development of industry-specific compliance guidelines or models.<sup>76</sup>

#### 9. Business Associates and other arrangements standard

This standard requires covered entities to obtain satisfactory assurances from business associates that the business associate will properly safeguard any electronic protected health information that is created, received, maintained or transmitted on behalf of the covered entity.<sup>77</sup>

The business associate standard replaces the “Chain of Trust” requirement in the proposed Rule. The terminology and requirements were changed in the Final Security Rule in order to coincide with the Privacy Rule requirements.

As with the Privacy Rule, the Security Rule’s business associate requirements do not apply to the following transmissions of electronic protected health information:

- (1) Transmissions to a provider for treatment purposes;
- (2) Transmissions of information from a group health plan, HMO, or other insurance issuer to a plan sponsor to the extent that the appropriate amendments to the plan documents have been made; and
- (3) Transmission of information from a health plan that is a government agency to another agency, if the other agency is responsible for making enrollment decisions or collecting data related to enrollment decisions and the sharing of information for such purposes is authorized by law.<sup>78</sup>

##### *a. Written contract or other arrangement*

Similar to the requirements imposed by the Privacy Rule, this standard contains a required implementation specification of “written contract or other arrangement.”<sup>79</sup> Specifically, the covered entity must obtain required satisfactory assurances by entering into an agreement with the business associate, whereby the business associate agrees that it will: (1) implement administrative, physical, and technical safeguards to protect electronic protected health information in accordance with the Security Rule; (2) ensure that the business associate’s agents or subcontractors who receive electronic protected health information also agree to implement reasonable and appropriate safeguards with respect to the electronic protected health information; (3) report to the covered entity any security incident of which it becomes aware; and (4) authorize termination of the contract by the covered entity if the business associate violates a material term of the agreement.<sup>80</sup>

---

<sup>76</sup> 68 Fed. Reg. 8352

<sup>77</sup> 45 CFR §164.308(b)(1)

<sup>78</sup> 45 CFR §164.308(b)(2); 45 CFR §164.502(e)(1)(ii)(C)

<sup>79</sup> 45 CFR §164.308(b)(4)

<sup>80</sup> 45 CFR §164.314(a)(2)(i)

Thus, covered entities who have recently entered into business associate agreements in order to comply with the Privacy Rule's April 14, 2003 deadline, will now be required to make additional amendments to many of these agreements prior to the Security Rule deadline. Covered entities should be reminded that, even if they do not provide the business associate with protected health information in electronic format, the Security Rule would apply if the business associate creates electronic protected health information on behalf of the covered entity. For example, if a covered entity provides a billing company with hard copy information, the parties will need to enter into a business associate agreement containing the required security provisions if the billing company converts this information into electronic format prior to submission to a payor.

Where a covered entity and its business associate are both governmental entities, the entities need only enter into a "memorandum of understanding" containing terms designed to meet the same objectives as those contained in the business associate contract. A memorandum of understanding is not necessary if the business associate is subject to another law that contains requirements that would meet the objectives of the memorandum of understanding.<sup>81</sup>

Likewise, when a business associate is required by law to perform functions or services on behalf of a covered entity, the covered entity only needs to document that good faith efforts were made to obtain satisfactory assurances from the business associate in a memorandum of understanding as discussed above.<sup>82</sup> HHS also noted that if a covered entity or a business associate is under a statutory obligation that would prevent either party from terminating an agreement to provide services, then the termination provision may be omitted from the business associate agreement.<sup>83</sup>

### ***Physical Safeguards: Standards and Implementation Specifications***

The Final Security Rule defines physical safeguards as "physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion."<sup>84</sup> There are four required standards that fall within this category.

#### **1. Facility Access Controls Standard**

This standard requires covered entities to implement policies and procedures to limit physical access to electronic information systems, as well as the facilities in which the systems are housed. In addition, this standard requires the covered entity to ensure that properly authorized access is allowed.<sup>85</sup> For purposes of the Security Rule, "facility" is

---

<sup>81</sup> 45 CFR §164.314(a)(2)(ii)(A)

<sup>82</sup> 45 CFR §164.314(a)(2)(ii)(B)

<sup>83</sup> 45 CFR §164.314(a)(2)(ii)(C)

<sup>84</sup> 45 CFR §164.304

<sup>85</sup> 45 CFR §164.310(a)(1)

defined as “the physical premises and interior and exterior of a building(s).”<sup>86</sup> This standard contains four addressable implementation specifications.

*a. Contingency operations*

The first addressable implementation specification is “Contingency operations”. This specification, if addressed, requires covered entities to establish policies and procedures which would allow appropriate access to the facility in the event of an emergency so that the disaster recovery plan and the emergency mode operations plan, developed under the administrative safeguards section, can be carried out to restore lost data.<sup>87</sup>

*b. Facility security plan*

“Facility security plan” is the next addressable implementation specification. This specification would involve the implementation of policies and procedures to safeguard the facility and the equipment contained within the facility from unauthorized access, tampering, and theft.<sup>88</sup> HHS notes that where a covered entity occupies only a portion of a building, facility security must still be addressed. A covered entity that implements a facility security plan should include in its plan any facility security measures undertaken by a third party, such as a lessor.<sup>89</sup>

*c. Access control and validation procedures*

The third addressable implementation specification under the facility access controls standard is “Access control and validation procedures”.<sup>90</sup> This specification is similar to the access authorization specification under the administrative safeguards category. However, this specification would provide for the implementation of procedures to control and validate a person’s access to the facility itself, or specific portions of the facility where electronic protected health information is housed. The level of access should be based upon an individual’s role or function.<sup>91</sup> For example, the covered entity might limit access to an equipment room that houses the facility’s mainframe computer. Policies and procedures should also address visitor control, such as requirements for visitor sign-in sheets or supervision. The establishment of access to software programs for those individuals involved in testing and revision should also be addressed.<sup>92</sup>

*d. Maintenance records*

The final addressable implementation specification under this standard is “Maintenance records”. This specification would include the implementation of policies and procedures to document those repairs or modifications performed on facility components that are

---

<sup>86</sup> 45 CFR §164.304

<sup>87</sup> 45 CFR §164.310(a)(2)(i)

<sup>88</sup> 45 CFR §164.310(a)(2)(ii)

<sup>89</sup> 68 Fed. Reg. 8353

<sup>90</sup> 45 CFR §164.310(a)(1)(iii)

<sup>91</sup> Id.

<sup>92</sup> Id.

related to physical security. For example, a covered entity's policies and procedures might address keeping a log of repairs or modifications made to the facility's hardware, walls, doors, and locks.<sup>93</sup>

## 2. Workstation Use Standard

This standard requires covered entities to implement policies and procedures specifying the functions that workforce members are permitted to perform on their individual workstations, and the appropriate manner in which these functions should be carried out. Policies and procedures developed pursuant to this standard must also address the physical attributes of the surroundings of workstations with access to electronic protected health information.<sup>94</sup> The term "workstation" as used in the Final Security Rule means "an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment."<sup>95</sup> An example of a policy related to workstation use would be a requirement that employees log off of a computer before leaving it unattended.<sup>96</sup>

## 3. Workstation Security Standard

This standard requires covered entities to implement policies and procedures to limit access to workstations to those individuals who are authorized to use the workstation.<sup>97</sup> The specific measures that will be taken will be dependent on the covered entity's risk analysis and risk management process.<sup>98</sup> For example, a small provider with a single workstation that is shared by employees with equal access will have fewer issues to address than a large organization with many workstations and varying levels of access.

## 4. Device and Media Controls Standard

This standard requires covered entities to implement policies and procedures related to moving hardware and electronic media into the facility, out of the facility, and within the facility.<sup>99</sup> The standard includes two required and two addressable implementation specifications.

### *a. Disposal*

The first required implementation specification is "disposal". This specification requires covered entities to implement policies and procedures dealing with the safeguarding of electronic protected health information that is being disposed of, including the disposal of

---

<sup>93</sup> 45 CFR §164.310(a)(1)(iv)

<sup>94</sup> 45 CFR §164.310(b)

<sup>95</sup> 45 CFR §164.304

<sup>96</sup> 68 Fed. Reg. 8354

<sup>97</sup> 45 CFR §164.310(c)

<sup>98</sup> 68 Fed. Reg. 8354

<sup>99</sup> 45 CFR §164.310(d)

hardware or other media containing such information.<sup>100</sup> For example, policies and procedures might deal with the erasure of computer hard drives prior to disposal.

*b. Media re-use*

Similarly, the second required implementation specification, “Media re-use”, would require policies and procedures addressing the erasure of protected health information from electronic media that is being re-used.<sup>101</sup> For example, a covered entity that puts electronic protected health information on floppy disks might develop a policy requiring the erasure of all floppy disks prior to re-use.

*c. Accountability*

The “Accountability” implementation specification is addressable and involves the maintenance of a record of the movement of hardware and electronic media and the documentation of persons responsible for such movement.<sup>102</sup> In the preamble to the Final Security Rule, HHS discusses an example of a manual record system where the movement of hardware and electronic media is limited to certain individuals and a log is kept of all such movement.<sup>103</sup>

*d. Data backup and storage*

“Data backup and storage” is the final addressable implementation specification under the device and media controls standard. This specification, if implemented, would require covered entities, prior to moving any equipment, to create a retrievable exact duplicate copy of all electronic protected health information housed on the equipment.<sup>104</sup>

***Technical Safeguards Standards and Implementation Specifications***

The proposed Rule contained technical security services requirements and separate requirements for technical security mechanisms, which were specific to information transmitted over a network.<sup>105</sup> These requirements were consolidated in the Final Rule under the heading of Technical safeguards.<sup>106</sup> Technical safeguards are defined in the Final Rule as “the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.”<sup>107</sup> The technical safeguards standards will be the portion of the Rule that will most likely require the input of IT staff or technological consultants and vendors.

**1. Access Control Standard**

---

<sup>100</sup> 45 CFR §164.310(d)(2)(i)

<sup>101</sup> 45 CFR §164.310(d)(2)(ii)

<sup>102</sup> 45 CFR §164.310(d)(2)(iii)

<sup>103</sup> 68 Fed. Reg. 8354

<sup>104</sup> 45 CFR §164.310(d)(2)(iv)

<sup>105</sup> 68 Fed. Reg. 8354

<sup>106</sup> 45 CFR §164.312

<sup>107</sup> 45 CFR §164.304

This standard requires covered entities to implement technical policies and procedures restricting access to electronic protected health information to those persons who have been granted access, pursuant to the Information access management standard.<sup>108</sup> Thus, while the Information access management standard involves the decision process regarding who should have access, the Access control standard requires covered entities, through the use of technology, to restrict the access accordingly. Specific technologies will be dependent on the outcome of the risk management and risk analysis and must take into account the general requirements or goals of the Security Rule. This standard contains two required and two addressable implementation specifications.

*a. Unique user identification*

Pursuant to the first required implementation specification, “Unique user identification”, covered entities are required to give all users a unique name and/or number for identifying and tracking the user’s identity.<sup>109</sup> Although this specification clearly requires assignment of a unique identification name or number, it is unclear whether users would be prohibited under all circumstances from accessing electronic protected health information under a generic username. For example, in small provider offices it is common practice for the patient scheduling system to be housed on one computer, with more than one individual sharing the responsibility of inputting and retrieving patient scheduling information. This specification would require individuals to continually log in and out of the system when registering and scheduling patients, despite the fact that all users have equal access.

In addition, it is unclear how detailed the “tracking” component of this implementation specification must be. While the proposed Rule specifically required audit trail capabilities as an implementation feature, the Final Rule deletes this specific requirement and instead includes it as part of the Access control standard.<sup>110</sup> Based upon HHS’ representations that the Final Rule is intended to be flexible and scalable for all sizes of entities, it would seem unreasonable to impose the financial burden of a new system on a small provider whose current software does not specifically track the details of each user’s access.

*b. Emergency access procedure*

The second required implementation specification under this standard is “Emergency access procedure”, which requires covered entities to adopt policies and procedures setting forth the ways in which access to necessary electronic protected health information can be obtained during emergencies, such as power outages related to natural or manmade disasters.<sup>111</sup> In developing these policies and procedures, covered entities

---

<sup>108</sup> 45 CFR §164.312(a)(1); 45 CFR §164.308(a)(4)

<sup>109</sup> 45 CFR §164.312(a)(2)(i)

<sup>110</sup> 68 Fed. Reg. 8356

<sup>111</sup> 45 CFR §164.312(a)(2)(ii); 68 Fed. Reg. 8355

should think through which electronic protected health information would be necessary for continuation of patient care and what alternatives exist for gaining access.

c. *Automatic logoff*

“Automatic logoff” is an addressable implementation specification that was a required implementation feature under the proposed Rule. This specification involves electronic procedures to automatically disconnect a user from an electronic session after a predetermined period of inactivity.<sup>112</sup> HHS recognized that this requirement was too specific and that alternative measures would be permitted based upon the covered entity’s risk assessment.<sup>113</sup>

d. *Encryption and decryption*

“Encryption and decryption” is another implementation specification that was required under the proposed Rule, but was designated as addressable in the Final Rule. This specification involves the implementation of mechanisms to encrypt and decrypt electronic protected health information in order to prevent unauthorized access.<sup>114</sup> HHS recognized that this was not necessary in all situations, and, depending on the risk assessment of the covered entity, could be addressed by alternative means. Specifically, HHS states in the preamble that encryption may not be necessary for “data at rest”, depending on the covered entity’s risk analysis.<sup>115</sup>

2. Audit Controls Standard

This standard requires covered entities to implement a mechanism to record and examine activity in information systems that contain or use electronic protected health information. The mechanism may be through hardware, software, or procedural mechanisms.<sup>116</sup> A covered entity has flexibility in determining how to implement this standard in a manner that is appropriate considering its risk assessment.<sup>117</sup>

3. Integrity Standard

This standard requires covered entities to implement policies and procedures to protect against the improper alteration or destruction of electronic protected health information.<sup>118</sup>

a. *Mechanism to authenticate electronic protected health information*

---

<sup>112</sup> 45 CFR §165.312(a)(2)(iii)

<sup>113</sup> 68 Fed. Reg. 8355

<sup>114</sup> 45 CFR §164.312(a)(2)(iv)

<sup>115</sup> 68 Fed. Reg. 8355

<sup>116</sup> 45 CFR §164.312(b)

<sup>117</sup> 68 Fed. Reg. 8355

<sup>118</sup> 45 CFR §164.312(c)(1)

The standard includes only one addressable implementation specification, “Mechanism to authenticate electronic protected health information” which would involve the implementation of “. electronic mechanisms designed to corroborate that the electronic protected health information has not been altered or destroyed.”<sup>119</sup> In response to commenters’ concerns that authentication would be too burdensome for much of the industry, HHS noted that certain authentication mechanisms, such as error-correcting memory and magnetic disc storage, are already commonly used within the health care industry.<sup>120</sup> HHS further noted that the covered entity’s risk analysis and risk management process would be used to determine which data needed to be authenticated.<sup>121</sup>

#### 4. Person or Entity Authentication Standard

This standard requires covered entities to “implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.”<sup>122</sup> To achieve this end, the proposed Rule would have required both automatic logoff and unique user identification, in addition to one of the following: (1) a biometric identification system; (2) a “password” system; (3) a “personal identification number”; and (4) “telephone callback” or a “token” system that uses a physical device for user identification.<sup>123</sup>

The Final Rule maintains only the general requirement that a mechanism be put in place to authenticate the identity of the person or entity, without specifying any particular measures. HHS notes that the mechanisms in the proposed Rule, as well as many other mechanisms, could be used to implement this standard.<sup>124</sup>

#### 5. Transmission Security Standard

This standard requires covered entities to implement security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.<sup>125</sup> The standard contains two addressable implementation specifications.

##### *a. Integrity Controls*

Integrity controls is an addressable specification which would involve the implementation of security measures to ensure that electronic protected health information that is transmitted electronically is not improperly modified without detection.<sup>126</sup>

---

<sup>119</sup> 45 CFR §164.312(c)(2)

<sup>120</sup> 68 Fed. Reg. 8356

<sup>121</sup> *Id.*

<sup>122</sup> 45 CFR §164.312(d)

<sup>123</sup> 68 Fed. Reg. 8356

<sup>124</sup> *Id.*

<sup>125</sup> 45 CFR §164.312(e)(1)

<sup>126</sup> 45 CFR §164.312(e)(2)(i)

*b. Encryption*

Encryption is also an addressable implementation specification under this standard and would involve the implementation of a mechanism to encrypt electronic protected health information whenever deemed appropriate.<sup>127</sup>

In the proposed Rule, encryption would have been mandatory whenever information was transmitted across “the Internet or dial-up connections.” HHS agreed with numerous commenters that the risk of interception over a dial-up line is very small, and, thus, encryption should not be mandatory. With respect to transmission of information over the Internet, HHS continues to encourage the use of encryption technology, although it is not mandatory.<sup>128</sup> Covered entities are required to encrypt transmissions when determined appropriate based upon the covered entity’s own risk analysis.<sup>129</sup>

HHS also addressed commenters’ concerns regarding the covered entity’s obligations with respect to unsolicited electronic protected health information received in an unsecured manner, such as an e-mail from a patient. With respect to such information, it is the covered entity’s obligation to afford appropriate security protection to this information once it is in possession of the covered entity.<sup>130</sup>

***Requirements for Group Health Plans***

Similar to the Privacy Rule, the Security Rule permits a group health plan to disclose electronic protected health information to the plan sponsor, only if the plan documents have been amended.

The amendments required by the Security Rule include the incorporation of provisions requiring the plan sponsor to: (1) implement safeguards in compliance with the Security Rule; (2) ensure that the adequate separation required by the Privacy Rule is supported by reasonable and appropriate security measures; (3) ensure that any agent or subcontractor to whom it provides information agrees to implement reasonable and appropriate security measures; and (4) report to the group health plan any security incident of which it becomes aware.<sup>131</sup>

***Documentation Requirements***

Similar to the Privacy Rule, the Final Security Rule requires covered entities to maintain written policies and procedures to comply with the requirements of the Security Rule.<sup>132</sup> The policies and procedures may be maintained in hard copy or electronically, must be made available to those persons who are responsible for implementing the procedures,

---

<sup>127</sup> 45 CFR §164.312(e)(2)(ii)

<sup>128</sup> 68 Fed. Reg. 8357

<sup>129</sup> Id.

<sup>130</sup> Id.

<sup>131</sup> 45 CFR §164.314 (b)

<sup>132</sup> 45 CFR §164.316(b)(1)(i)

and must be retained for at least six years.<sup>133</sup> Policies and procedures must be reviewed and updated periodically in order to address environmental or operational changes affecting the security of electronic protected health information.<sup>134</sup>

Covered entities must also maintain for six years any paper or electronic documentation of any activity, action or assessment that is required by the Security Rule.<sup>135</sup>

The Final Rule removes the term “formal” from the documentation requirements because of the concern that the connotation was stricter than intended by the Rule. HHS does make clear that official organization statements are required, rather than “word of mouth” or “cryptic notes scratched on a notepad.”<sup>136</sup>

### ***Compliance Deadlines***

The deadline for compliance with the Security Rule is April 20, 2005, with the exception of small health plans who will need to be in compliance by April 20, 2006.<sup>137</sup> The definition of small health plan is the same as that set forth in the Privacy Rule and includes those health plans with annual receipts of five million dollars or less.<sup>138</sup>

### ***Sources for More Information***

HHS refers throughout the Security Rule to publications authored by the National Institute of Standards and Technology (NIST). In addition, HHS stated that NIST is undertaking the certification of software and off-the-shelf products for compliance with the Security Rule.<sup>139</sup> The website for NIST is <http://www.niap.nist.gov>. HHS also referenced the Workgroup for Electronic Data Interchange’s (WEDI) Strategic National Implementation Process (SNIP) organization’s website for further information regarding voluntary regional organizations that have been formed for the purpose of addressing HIPAA issues. The SNIP/WEDI website is <http://www.snip.wedi.org>.

### ***Summary***

Although covered entities have some time to achieve compliance with the Final Security Rule, they are well advised to immediately begin reviewing and understanding the Rule’s requirements and obligations. As the Security Rule is complex and involves technical as well as legal and risk assessment aspects, health care attorneys should play an important role in assisting covered entity clients in achieving compliance.

---

<sup>133</sup> 45 CFR §164.316(b)(2)

<sup>134</sup> 45 CFR §164.316(b)(2)(iii)

<sup>135</sup> 45 CFR §164.316(b)(1)(ii)

<sup>136</sup> 68 Fed. Reg. 8349

<sup>137</sup> 45 CFR §164.318

<sup>138</sup> 45 CFR §160.103

<sup>139</sup> 68 Fed. Reg. 8352