DAVIS WRIGHT TREMAINE LLP ANALYSIS & COMMENTS
ON HHS'S JUST-RELEASED HIPAA SECURITY RULES
Richard D. Marks, Paul T. Smith, Thomas E. Jeffry, Jr., Rebecca L. Williams
http://www.ehealthlaw.com

WASHINGTON, DC USA -- MEDICAL INDUSTRY E-MAIL NEWS SERVICE(TM) – FEB. 17, 2003 -- Four years and 11 months ago the statutory deadline (February 28, 1998) passed for the Secretary of Health and Human Services (HHS) to issue the HIPAA security rules in final form. Now we have the rules. They were released in prepublication form on February 13, and the official version is expected to appear in the Federal Register on February 20, 2003. After the 60-day period mandated by the Congressional Review Act and 24 months mandated by the HIPAA statute, the security rules will become effective for enforcement purposes in April 2005. The new security rules can be downloaded from the CMS website at www.cms.gov.

INITIAL IMPACT

The 2005 effective date tells only part of the story. The "mini-security rule" in the HIPAA *privacy* rules (45 CFR 164.530(c)) goes into effect in less than two months. It requires covered entities and their business associates, as of April 14, 2003, to implement "appropriate administrative, technical and physical safeguards" for protected health information in all forms, non-electronic and electronic. It is likely that the meaning of "appropriate safeguards" under the privacy rules will in part be determined by referring to the general principles (if not all the specific requirements) of the new final security rules. Viewed in this perspective, the first impact of the new security rules is almost immediate.

OVERVIEW – A BRIEF COMPARISON TO THE PROPOSED SECURITY RULES

The document released by HHS contains the rules and a long explanatory preamble. For those of you who need to read the entire document, we suggest that you go first to the back, to page 245, and start with the rules themselves (45 typed pages). Then go back to the beginning of the document to read the 244-page preamble. Things will fall into place faster.

The new security rules fulfill HHS's oft-repeated promise to mesh the security rules and the HIPAA privacy rules. The new rules discard much of the proposed security rules' terminology in favor of definitions in common with the privacy rules. For example, the requirements of a "chain of trust" agreement in the proposed security rules are now additional "business associate" contract requirements.

Some changes in terminology were made simply for the sake of consistency with the privacy rules. Others reflect a shift in substance too, such as the change from security "certification" to "evaluation," or the shift from "information access control" to "information access management," a broader concept. Other modifications to terminology introduce a new concept, approach, or new emphasis, such as the rules for "media re-use procedures."

The proposed security rules were organized around four overlapping categories (administrative procedures, physical safeguards, protection for data at rest, and protection for data in transit). Describing these overlaps often produced confusing redundancy, both in the proposed security rules themselves and in analysis of the proposed rules. The new rules retain the core concepts found in the old four categories – essentially, the basic building blocks of security – but eliminate the four silos. This streamlines the security rules in comparison to what was proposed.

Generally speaking, the final security rules offer less detail and more generic guidance, in the sense of high-level direction, about how covered entities and their business associates should go about implementing security. As HHS says, "we have focused more on what needs to be done and less on how it should be accomplished."

This means that the new rules are less a series of checklists and more a description of principles for each covered entity and business associate to evaluate and apply, based on the entity's specific situation. One benefit to this approach, as a general matter, is less regulatory risk through the enforcement process. Other risks remain however, because of the new rules' demands on covered entities to exercise constant vigilance and apply prudent judgment about security to changing circumstances. These are familiar litigation risk management issues.

The new security rules' scope is narrowed to protected health information (PHI) in electronic form only. Consequently, many details of implementing the security rules may not apply to PHI that is not in electronic form. However, HHS emphasizes that the privacy rules apply to PHI in any form. The reader should remember the "mini-security rule" in the HIPAA *privacy* rules (45 CFR 164.530(c)), discussed above. It requires that "appropriate" security be applied to all PHI in any event, whether or not the security rules themselves apply.

One area of vast improvement is the final security rules' explicit recognition that the cost of implementing security is a factor in security decisions (and, presumably, in regulatory and judicial judgments about security issues). The entire health care industry benefits from this dose of realism, and small and rural providers especially benefit. Indeed, the new security rules and their preamble repeatedly recognize that the cost of security is a major factor for small offices and facilities and those in rural areas. At the same time, HHS cautions that cost considerations do not justify ineffective security. "[T]here is a clear requirement that adequate security measures be implemented . . . . Cost is not meant to free covered entities from this responsibility."

Despite this caution, the new rules are a marked improvement in meeting the command in the HIPAA statute that cost of security must be factored into the new rules. Combined with discussions of operational scale that are a noticeable improvement from the proposed security rules, the new rules are likely to be far easier for small and rural health care providers to apply. While this approach does not eliminate all enforcement or litigation risk, it improves the regulatory climate substantially.

HHS creates a new Subpart C in Part 164, Volume 45 of the Code of Federal Regulations ("CFR"), where the HIPAA rules are officially published. The bulk of the new security rules are now in the new Subpart C. General provisions remain in Subpart A, and the privacy rule remains in Subpart E. Conforming changes are also made in two existing parts of the HIPAA rules, in Parts 160 and 162 of Volume 45 of the CFR. Parts 160 and 162 are rules (such as definitions) that apply to all the HIPAA rules – privacy and transactions, as well as security. These changes will simplify references to the HIPAA rules and make it easier to find specific rules. As we note below, some definitional provisions are removed from the privacy rule and placed in the general provisions of Subpart A, to make them applicable to the new security rule as well as the existing privacy rule.

The preamble states that future rulemaking proceedings will deal with enforcement of security and privacy, and separately with electronic signatures. HHS gives no timetable for either rulemaking.

STRUCTURAL ELEMENTS: STANDARDS AND REQUIRED AND ADDRESSABLE IMPLEMENTATION SPECIFICATIONS

The new rules have "standards" and "implementation specifications." Implementation specifications can be either "required" ("R") or "addressable" ("A"). Appendix A to the rules is a "Security Standards Matrix" that lists each standard and its associated implementation specifications. The matrix shows by an "R" or "A" whether the particular implementation specification is required or addressable, and lists the section of the security rules where the standard and implementation specification are found.

Essentially, a standard explains what must be done, and implementation specifications explain how to do it. If HHS believes that an implementation specification is one of many options, none of which by itself is essential, then it will label the implementation specification "addressable" ("A"). If HHS sees the implementation specification as essential, it will be "required" ("R").

In some case, a standard is sufficiently self-contained so that the means of its implementation are explicit or implicit, and without the need for any implementation specifications. For examples, readers should look at the rules on "assigned security responsibility" (164.308(a)(2)) or "workstation use" (164.310(b)).

The standards are grouped under three headings: Administrative Safeguards, Physical Safeguards, and Technical Safeguards. While there remains inevitable overlap, these categories prove more streamlined than the organization of the proposed security rules.

THINKING ABOUT SECURITY UNDER THE NEW RULES

The standards and implementation specifications are integral to how HHS wants covered entities and their business associates to think about security. The preamble reflects HHS's recognition (gleaned from comments filed about the proposed rule) that many in the health care industry found security perplexing.

HHS instructs that the place to start thinking about security under the new rules is section 164.306. This section is the heart of the new security rules, and tracks the part of the HIPAA statute that governs security standards and safeguards (42 USC 1320d-2). Covered entities must meet four security requirements specified in section 164.306(a):

> (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.
> (4) Ensure compliance . . . by its workforce.

Section 164.306(b) specifically calls for a flexible approach: "Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart." The rules allow covered entities to factor in cost, size, complexity, technical infrastructure, other capabilities, and the likelihood and seriousness ("criticality") of potential security risks.

Section 164.306(c) specifies that covered entities accomplish all this by reference to the standards and their associated implementation specification, whether required or addressable. If the standard has no implementation specifications, it can and must be implemented as the standard itself specifies. If there are required implementation specifications, then the covered entity must do what the specifications demand.

However, there is significant flexibility in approach because so many of the implementation specifications are addressable, not required. A covered entity must assess whether each addressable specification is reasonable and appropriate for its unique situation. Then it has choices. If the specification is reasonable and appropriate for that covered entity, it "must" be implemented. If it is not reasonable and appropriate, the entity must either implement another equivalent measure that is reasonable and appropriate or, if the standard can be met some other way, choose not to implement the specification or any equivalent specification. The covered entity must document the reasons for its choice.

Risk Assessment and Risk Management.

The preamble explains 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) of § 164.306(a)." The way a covered entity knows what measures are reasonable and appropriate to achieve each of the listed tasks is through a two-step process that is mandated in the new rules. The first step is to assess the security risks it faces. Then it must implement countermeasures proportional to those risks, and manage its countermeasures to keep up with new or increased risks.

HHS explains the requirement this way in the preamble: "Thus, an entity's risk analysis and risk management measures required by § 164.308(a)(1) must be designed to lead to the implementation of security measures that will comply with § 164.306(a)." Whether particular measures comply with the rules will be determined by their effectiveness in "ensuring" the confidentiality, integrity, and availability of PHI, and in protecting PHI against "any reasonably anticipated threat or hazard." By the way it has written section 164.306 and explained it in the preamble, HHS has set a high standard for security, and narrowed legal arguments about how to interpret the HIPAA statute's language about safeguards.

HHS refers several times to guides published by NIST, the National Institute of Standards and Technology, as an aid in risk assessment and in the security management process(discussed below). The NIST "800 Series" publications are important as practical guides that expand upon HHS's explanations of steps to follow, and criteria to use, in assessing risk and managing security implementation. The guides will also be important references in HHS's enforcement of the security rules and in other litigation over security issues.

The preamble's discussion of risk assessment and risk management will assist covered entities in understanding what they should do to achieve an appropriate level of security, how to make decisions about doing it, and how to document it. Documentation under the new rules will be a critical element in justifying a covered entity's approach to its security needs and the countermeasures it selects to meet them.

However, the new security rules only set out a process for decision-making. They do not make the decisions nor prescribe any particular technology. Indeed, the preamble is determinedly and explicitly technology-neutral. This is true for issues covering everything from how to protect workstations to whether or not encryption is appropriate in any given situation. Some examples are worth noting because they have been the subject of so much discussion since the proposed security rules appeared:

- The preamble explains which kinds of fax processes are "electronic" and which are not. The rationale for the explanation, we predict, will continue to be a source of controversy and bemusement. Generally speaking, paper-to-paper (old-style) faxes are not electronic, and computer faxes are electronic.

- Voice (*i.e.*, good old) telephone is not electronic.

- The rule disavows a distinction between data that moves internally within or externally to an organization. This is likely to lead many covered entities to assess the risks associated with their internal networks in a new light.

- The much-criticized proposal that workstations have required automatic log-off is a thing of the past. Workstation protection is now much more flexible in concept.

<u>Security Management Process</u>.

The new rules require covered entities and business associates to manage security processes assiduously. There is new emphasis, for example, on an entity's ability to detect an intrusion (such as a hacker attack) and respond quickly and effectively with countermeasures. This is known as "incident response." This and similar security management requirements will likely lead to integration of security processes and technology that are not yet common in health care. The expense of these precautions may well fall sooner and more heavily on larger health care organizations, because that is a natural result of the new rules' emphasis on scalability.

Training is one aspect of security management, and the new rules state that security training must be given to a covered entity's entire workforce, not just that part of the workforce that comes in contact with PHI. As with all aspects of the security management process, training must keep up with the times – with changes in threats and countermeasures.

No Safe Harbor.

The new security rules offer no safe harbor to covered entities, business associates, or the people who make security decisions for them. Rather, whether security countermeasures are good enough to "ensure" the confidentiality, integrity, and availability of PHI, and protect it from "any" hazard one could reasonably anticipate, is likely to be judged retroactively. Results and the documentation of decisions will both be important.

These considerations apply both to HHS's regulatory enforcement of security and privacy, and to covered entities' and business associates' management of litigation risk. Because the rules are based on the judgments involved in risk assessment and risk management, and on the effective implementation of the security management process, there is inherent exposure to legal liability. It cannot be eliminated, and the new rules do not attempt to do so.

SECURITY ASPECTS OF BUSINESS ASSOCIATE CONTRACTS

One of the requirements of the proposed rules was a "chain of trust partner agreement." This was the agreement by which two parties would agree to exchange electronic data and to protect it in the course of transmission. Its goal would be to ensure security at all points in the transmission, and it would have been required for all electronic transmissions of protected health information.

The privacy rules have a different requirement, the "business associate contract." This is an agreement that a covered entity is required to obtain from contractors – called business associates – who assist the covered entity with payment or operations, and who have access to the covered entity's protected health information. Under the privacy rules, a business associate contract is not universally required for exchanges of health information – for example, a provider needs one to disclose health information to a clearinghouse, but not to a health plan, because the clearinghouse is viewed as assisting the provider with payment, but the health plan is acting independently. Similarly, disclosures to providers for treatment do not require business associate contracts.

Observers have been interested to see how the final security rules would coordinate these differing requirements. They do it by abandoning the chain of trust partner agreement as a legal requirement. Instead, they require covered entities to have agreements with business associates who create, receive, maintain or transmit electronic protected health information on the covered entity's behalf. These agreements must contain assurances from the business associate that it will appropriately safeguard the information.

The security rules set forth the required assurances. They are a subset of the provisions required by the privacy rule, focused on electronic information. The business associate contract must require the business associate to:

- Implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the covered entity's electronic protected health information;

- Ensure that its agents and subcontractors to whom it provides the information do the same;

- Report to the covered entity any security incident of which it becomes aware.

The contract must also authorize termination if the covered entity determines that the business associate has violated a material term.

The security rules adopt the privacy rules' definition of "business associate." They also echo the privacy rules' exceptions to the contract requirement for disclosures to providers for treatment, exchanges of information between government entities, and exchanges between group health plans and their sponsors.

Interestingly, however, the security rules do not dispense with business associate contracts for covered entities participating in an organized health care arrangement, as the privacy rules do.

Likewise, the standard of liability is the same as under the privacy rules – a covered entity would not be liable for breaches by its business associate unless it knew of a pattern of activity or practice in violation of the agreement, and failed to take appropriate measures. Otherwise, covered entities who transmit data electronically will not be responsible for the recipient's security implementation.

The requirement that the business associate report any security incident of which it becomes aware to the covered entity makes it likely that covered entities will know about most, if not all, incidents. (The new security rules discard the term security "breach.") Further, security protocols require close coordination, so it is unlikely that covered entities and business associates will be able to maintain the business process or technical process separation that the new security rules seem to envision. We will need experience under the new rules before these apparent contradictions can be evaluated.

In every case in which the security rules would require a business associate contract, the privacy rules would too. Accordingly, the requirements of the security rules will most likely be implemented as additional provisions to the standard contract for business associates who deal with a covered entity's electronic protected health information.

Unlike the proposed chain of trust partner agreement, the business associate contract does not relate to the security of the data transmission itself, but rather to the security of data in the hands of the business associate. Moreover, many electronic transmissions of health information will not be subject to the business associate rule at all, such as transmissions between providers and health plans for payment. Neither the privacy rules nor the security rules now have any requirement for a contract between participants in transmissions such as these.

However, both the privacy rules in a general way, and the security rules more specifically, will require covered entities to ensure the security of electronic data transmissions, whether or not the recipient is a business associate. And participants in electronic data interchange will still need to agree on communications and security protocols, so trading partner agreements are likely to continue to be recommended practice. Prudence will argue for security risk analysis and ongoing risk management in the negotiation and implementation of these agreements.

SECURITY RULES FOR AFFILIATED ENTITIES, HYBRID ENTITIES, AND GROUP HEALTH PLANS

There are new provisions intended to align the security rules with the approach taken by the privacy rules to affiliated entities, hybrid entities and group health plans.

Under the privacy rules, covered entities under common ownership or control may designate themselves an "affiliated covered entity." An affiliated covered entity is treated as a single covered entity under HIPAA. This has a number of consequences, one of which is that the affiliated entity as a whole is responsible for HIPAA compliance by its participants.

Hybrid entities are entities that have covered and non-covered functions, and that elect to designate their covered functions (and, optionally, related business functions) as "health care components." If they do this, they need comply with the privacy rule only within their designated health care components. However, they must restrict the disclosure of protected health information to non-covered components as they would to third parties. If they do disclose health information to non-covered components, they must ensure that the non-covered components do not use or disclose the information in a manner that would violate the regulations.

The security rules remove the provisions relating to affiliated covered entities and hybrid entities from the privacy rules, place them in the general administrative simplification provisions, and make them applicable both to the security rules and the privacy rules. In effect, the responsibilities of affiliated covered entities and hybrid entities for the maintenance of electronic health information under the security

rules now track their responsibilities with respect to the use and disclosure of health information under the privacy rules.

Group health plans raise different issues. Here the concern of the privacy rules is to ensure that plan sponsors (typically employers) do not have access to the plan's health information for employment-related purposes. Accordingly, the privacy rules restrict a plan sponsor's access to health information from the group health plan. Generally, the sponsor may have access only to aggregate information, and to information about who has enrolled or disenrolled in the plan.

However, if the sponsor has administrative responsibilities, it may also have access to information it needs to administer the plan. The plan document must contain provisions that restrict the plan sponsor's use of the information to this purpose, and require adequate separation between the sponsor's operations as plan sponsor and as employer. These provisions resemble those of a business associate contract, but they are in the form of amendments to the plan documents.

The security rules now require that, if the plan sponsor has access to electronic health information (beyond summary plan information and enrollment information), the plan document must have provisions, similar to those already required by the privacy rules, requiring the employer as plan sponsor to implement reasonable and appropriate measures to secure electronic health information, and to implement the adequate separation requirement; to require the same of its subcontractors; and to report all security incidents to the group health plan.

Wherever these provisions are required to be in plan documents, the related provisions under the privacy rules will also be necessary. Accordingly, we expect that group health plans that share electronic health information with their plan sponsors may want to combine them into a single amendment.

IMPACT OF NEW SECURITY RULES ON RESEARCH

The new security rules alleviate some concerns that the research community had with the chain of trust concept in the old proposed rule. Under that concept, any research (or other) database holding PHI would have needed the same high level of security as at the hospital, doctor's office, or other place where the PHI originated.

In contrast, the preamble explains that the final security rules (and all their restrictions) apply only to researchers who are part of a covered entity, or who are within the health care component of a hybrid covered entity (essentially the same thing). As the preamble states: "Researchers who are not part of the covered entity's workforce and are not themselves covered entities are not subject to the standards." This is consistent with a later statement in the preamble that, "this final rule does not require noncovered [*sic*] entities to comply with the security standards."

We do not want to leave the impression from this summary that security or privacy concerns abate completely when PHI is disclosed (even pursuant to an authorization) to researchers who are not covered entities or not employed at covered entities. However, we do believe that the new security rules offer some welcome relief from the rigidity of the chain of trust concept as originally explained in the proposed security rule.

CONCLUSION

This is an overview of the new HIPAA security rules. There are many changes to definitions and concepts, and new definitions and requirements, that we do not mention because of space limitations. We expect to publish further advisories about HIPAA security as events unfold.

FOR FURTHER INFORMATION, PLEASE CONTACT:

Richard D. Marks
Davis Wright Tremaine LLP
1500 K Street NW, Suite 450
Washington, DC 20005-1272
202-508-6611
richardmarks@dwt.com

Paul T. Smith
Davis Wright Tremaine LLP
One Embarcadero Center, Suite 600
San Francisco, CA 94111-3611
415-276-6532
paulsmith@dwt.com

Thomas E. Jeffry, Jr.
Davis Wright Tremaine LLP
865 South Figueroa Street, Suite 2400
Los Angeles, CA 90017-2566
213-633-6882
tomjeffry@dwt.com

Rebecca L. Williams
Davis Wright Tremaine LLP
1501 4th Ave
Seattle WA 98101-1688
206-628-7769 phone
beckywilliams@dwt.com

Carol Pratt
Davis Wright Tremaine LLP
1300 SW Fifth Avenue, Suite 2300
Portland, OR 97201-5682
503-778-5279
carolpratt@dwt.com

Barrie K. Handy
Davis Wright Tremaine LLP
1501 4th Ave
Seattle WA USA 98101-1688
206-628-7404 phone
hipaa@dwt.com
http://www.ehealthlaw.com