Reprinted with permission from the *Privacy Laws & Business International Newsletter*, March/April 2003.

Getting a handle on the new HIPAA security regulation

The US healthcare industry is now faced with new security provisions issued under the Health Insurance Portability and Accountability Act. **Kirk Nahra** outlines the new regulation and discusses the impact it will have on healthcare providers.

On February 20th, 2003, the US Department of Health and Human Services (HHS) released the long awaited security rule under the Health Insurance Portability and Accountability Act (HIPAA). This is the third leg of the HIPAA "Administrative Simplification" trilogy, covering privacy, standardised electronic transactions and security.

The Security Rule will have a substantial effect on any entity participating in the healthcare system, not only the "covered entities" under the rule (including health plans, healthcare providers and healthcare clearinghouses), but also their vendors and business partners that provide critical services. This rule will also become part of the developing law and regulatory structure surrounding the privacy of sensitive customer/patient information.

For those directly affected by this rule, the key questions will involve process (eg. what steps need to be put in place, what decisions will result from the evaluative security process) and when should steps be taken (eg. do I have the full two years, or does the HIPAA Privacy Rule require/encourage me to move more quickly?). In order to provide a context for these issues, this article presents a brief summary of the critical components of the Security Rule, and an initial analysis of how covered entities need to follow this rule, including some of the strategy questions facing covered entities – and their business partners — who need to structure their operations to protect the security of protected health information (PHI).

BACKGROUND

Since the HHS published the "draft" Security Rule four and a half years ago in August 1998, the world has become a vastly different place. We have witnessed the entire "boom and bust" of the "Dot.Com" economy. The Year 2000 "crisis" raised enormous concerns, and then fizzled out. Wireless communications, using cell phones, Blackberry devices and other technologies, once almost unthinkable, are now commonplace. The events of September 11th have changed, perhaps permanently, the relative balance between privacy rights and security obligations.

For the healthcare industry, change has been equally as dramatic. Malpractice reform, HMO (Health Maintenance Organisation) litigation, ERISA (Employee Retirement Income Security Act) changes, rising costs and technological advances have all highlighted the business of providing health care.

This time period has also seen the evaluation and implementation of most of the enormous challenges of the HIPAA Administrative Simplification. The standard transaction rules (which cover the electronic exchange of administrative and financial health care transactions) have been defined (for the most part), and healthcare companies (having incurred enormous information technology costs due to Y2K) have now moved to revamp their billing and claim systems. Congress, recognising the difficulties in complying with these "standard" transactions – which the industry is finding are not really "standard" – provided an extra year to achieve compliance – and the industry awaits to see whether the "standardised" system will actually work in October 2003 (the compliance date for the transaction rule).

On the privacy front - through two Administrations, various drafts, a final rule, and now a "Final" final rule - the industry is on the verge of the privacy compliance date, with respected advisory bodies predicting a "likelihood of widespread disruption" surrounding the April 14th 2003 compliance date.

Now, with only a few weeks to go on the privacy compliance front, the HHS has launched another "Administrative Simplification" landmine, the Security Rule – with wide-ranging effects not only on the security of electronic protected health information, but also with significant implications immediately for privacy compliance.

WHAT DOES THE SECURITY RULE SAY?

Prior to the Final Rule - The Security Rule provisions are not the first to set forth security requirements for the healthcare industry. The HIPAA statute, which has led to the creation of all of the Administrative Simplification provisions, contained specific requirements for the security of health-related information - effective in 1996. Specifically, the statute itself stated that:

> "Each [Covered Entity] who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical and physical safeguards:
>
> (a) to ensure the integrity and confidentiality of the information

> (b) to protect against any reasonably anticipated threats or hazards to the security or integrity of the information; and unauthorised uses or disclosures of the information; and
>
> (c) otherwise to ensure compliance with this part by the officers and employees of such [covered entity]" **- Title 42 United States Code 1320d-2(d)(2).**

Beyond this mandate – which required certain steps from the covered entities themselves, independent of the issuance of a Security Rule – the statute also required the Secretary of the US Department of Health and Human Services to adopt security standards that take into account:

> (i) the technical capabilities of record systems used to maintain health information
>
> (ii) the costs of security measures
>
> (iii) the need for training persons who have access to health information
>
> (iv) the value of audit trails in computerised record systems; and
>
> (v) the needs and capabilities of small healthcare providers and rural health care providers - **Title 42 United States Code 130d-2(d)(1)(A).**

Additionally, the same covered entities have been struggling to understand the security implications of the HIPAA Privacy Rule. Under the Privacy Rule's cryptic provisions, a covered entity "must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information" - **Privacy Rule, 45 CFR 164.530(c)(1)**. In addition, any "business associate" under the Privacy Rule (essentially, vendors to healthcare entities whose work involves patient/member information) must also agree by contract to "use appropriate safeguards to prevent use or disclosure of [PHI] other than as provided for by" the business associate contract. There is essentially no additional detail in the rule itself, or the preamble, as to what should be included in these "safeguards."

The Final Security Rule - While the Privacy Rule provisions are "separate" from the Security Rule – most importantly in terms of compliance dates – there are critical links. For example, according to the preamble:

> "[S]ecurity and privacy are inextricably linked. The protection of the privacy of information depends in large part on the existence of security measures to protect that information...
>
> The security standards...define administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic protected health information...The Privacy Rule, by contrast, set standards for how protected health information should be controlled by setting forth what uses and disclosures are authorised or required and what rights patients have with respect to their health information" **- Preamble to Security Rule, 68 Fed. Reg. at 8335.**

Moreover, in announcing the final Security Rule, the HHS also indicated that:

> "It is likely that covered entities will meet a number of the requirements in the security standards through the implementation of the privacy requirements. For example, in order to comply with the Privacy Rule requirements to make reasonable efforts to limit the access of members of the workforce to specified categories of protected health information, covered entities may implement some of the administrative, physical, and technical safeguards that the entity's risk analysis and assessment would require under the Security Rule. 68 Fed. Reg. at 8371."

In setting out the Security Rule requirements, the HHS focused on four key goals/mandates for covered entities. To be in compliance with this rule, a covered entity must:

> • ensure the confidentiality, integrity, and availability of electronic protected health information that is created, received, maintained, and transmitted
>
> • protect against "reasonably anticipated threats or hazards" to "security or integrity" of this information
>
> • protect against "reasonably anticipated uses or disclosures" of this information that are not permitted under the Privacy Rule; and
>
> • ensure compliance by its workforce.

In order to make this mandate feasible, the HHS developed a "flexible" approach to compliance by making the requirements "scalable" based on the specific nature of the organisation. The provisions are also intended to be "technology-neutral" – meaning that the rule does not dictate any specific technological solution. Instead, the rule focuses on process - how to evaluate a company's security risks and decide what steps should be taken.

Covered entities therefore, must develop appropriate security measures based upon:

> • the size, complexity, and capabilities of the covered entity
>
> • the covered entity's technical infrastructure, hardware, and software security capabilities
>
> • the costs of particular security measures; and
>
> • the probability and criticality of potential risks to electronically protected health information.

In general, with this "flexibility", a covered entity under the rule may use "any security measures that allow the covered entity to reasonably and appropriately implement the standards and specifications" of the Security Rule.

In addition, the rule breaks down the regulatory provisions into "standards" – which constitute the general security topic that must be addressed, and "specifications", which are the particular safeguards designed to address the specific standard. All of these issues are designed to protect "electronic" protected health information (eg. PHI from the Privacy Rule that is transmitted or maintained in electronic media. Some of the specifications are "Required" and must be implemented. Others are "addressable" meaning that a covered entity must review the issue and evaluate whether the particular step is "reasonable and appropriate" for implementation.

The rule sets out a series of "administrative" safeguards that constitute the key provisions of an effective security programme. In particular, the requirements for "risk analysis" and "risk management" set the stage for the remainder of the activities. In fact, most of the Security Rule describes an appropriate "process" that covered entities must go through in evaluating security options, which is broken down into technical, physical and administrative safeguards.

• Under the Rule, "risk analysis" means to: "Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity."

• Under the Rule: "risk management" involves an obligation to: "Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with [the Security Rule]."

Also included in the administrative safeguards are requirements such as a sanction policy, assigned responsibility for security activities, security awareness and training, contingency planning and "security incident" procedures (a "security incident" is an "attempted or successful unauthorised access, use, disclosure, modification or destruction of information or interference with system operations in an information system").

There is a separate administrative safeguard related to "business associates", which are vendors to covered entities (as defined by the HIPAA Privacy Rule). These security provisions will require specific provisions for business associate relationships (and, unfortunately, will require in most circumstances that covered entities amend the contracts they have already signed with business associates setting forth the requirements of the Privacy Rule).

"Physical" safeguards are less dramatic, but constitute an additional core set of safeguards. These include facility access controls (limiting physical access to information systems), workstation use policies, workstation security, and device and media controls (such as procedures for disposal of computer hardware in light of recent reports of privacy violations involving discarded computers that still retain PHI).

The "technical" safeguards also are relatively specific, involving access controls (such as unique user identification, automatic log-off, and emergency access procedures), audit controls, integrity (protection against improper alteration or destruction of PHI), person/entity authentication and transmission security.

In addition to these safeguards, the Security Rule requires covered entities to develop security policies and procedures, and to maintain appropriate documentation of these policies and procedures.

CRITICAL CHALLENGES AND CONCLUSIONS

With this background, what should companies in the healthcare industry be focusing their attention on over the next few months and years in connection with the security of health information?

Privacy connections: Regulatory requirements - One of the critical challenges involves what to do now about security, based on the requirements of the Privacy Rule. Clearly, the Privacy Rule requires all covered entities to take some steps to protect security. Moreover, unlike the Security Rule, the Privacy Rule security requirements are not limited to electronic information, and therefore require steps to protect all forms of protected health information. These steps should be in place as of April 14th 2003 for any covered entity.

> Healthcare entities need to view information security as an ongoing challenge, with today's industry standards quickly replaced by new templates.

Tension between access/privacy and security - As with all security rule provisions, regardless of the industry, the HIPAA security provisions also reflect a tension with one key component of most privacy rules – individuals' right to access information held on them. The easier the access, the "looser" the security protection. This is particularly important for companies that thrive on the Internet or other key forms of access to information on products. All covered entities will need to develop an effective balance between access and security, to reduce tensions between these privacy and security provisions.

Business associate issues - Covered entities that are currently completing their business associate contracting now face an additional bureaucratic hurdle – implementing the contracting requirements of the security rule. While the Security Rule require provisions that are very similar to terms that are mandated under the Privacy Rule, they are not the same (couldn't the HHS have done a better job on this?). Accordingly, covered entities will, in most instances, need to develop a second round of BA (Business Associate) contracting to incorporate security rule requirements.

Between now and 2005 - Perhaps the most immediate question for healthcare entities is how to interpret the Security Rule provisions now, while developing the Privacy Rule's "appropriate standards". Will security standards under the Privacy Rule be "appropriate" even if they are not what is

required by the Security Rule? Given the "post hoc" enforcement of most security concerns (meaning that enforcement happens only after there is a problem), will covered entities be able to maintain the position that their security is appropriate now, but under lesser standards than are required by the Security Rule? The HHS clearly did not intend to impose the security rule requirements immediately, but nor did they act aggressively to ensure that this result will not happen. The issue arises not only with general security provisions, but also in the context of a business associate contract. If there are business associate contracts that are not yet signed (and we know there are many), should covered entities move to include security rule provisions now, to avoid a second round of large-scale contracting in two years time? Can these provisions be written in a way that does not require premature compliance with the Security Rule?

CONCLUSION

With all these challenges, healthcare entities face an ongoing problem of how best to protect the customer/patient information entrusted to their care. How will these standards evolve between now and 2005? Obviously, healthcare entities today encounter a vastly different environment than when the draft security rule was issued in August 1998. While we may not see quite as much change in the computerised world in the next two years, healthcare entities need to view information security as an ongoing challenge, with today's industry standards quickly replaced by new templates. These companies also need to begin security efforts now and need to make security protection a continuing part of any healthcare entity's ongoing business operations.

AUTHOR: Kirk J Nahra is a partner with Wiley Rein & Fielding, LLP in Washington, DC, where he specialises in privacy/security litigation and counseling for a wide variety of insurers, healthcare payers and others. He received his law degree from Harvard Law School, Cum Laude, and his undergraduate degree from Georgetown University, magna cum laude and Phi Beta Kappa, in 1984. He is also the editor of *Privacy Officers Adviser*. He can be reached at Tel: +1 202 719 7335, or E-mail: knahra@wrf.com.

HIPAA: See the US Department of Health and Human Services website: www.hhs.gov/ocr/hipaa