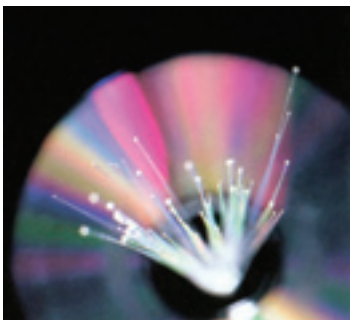
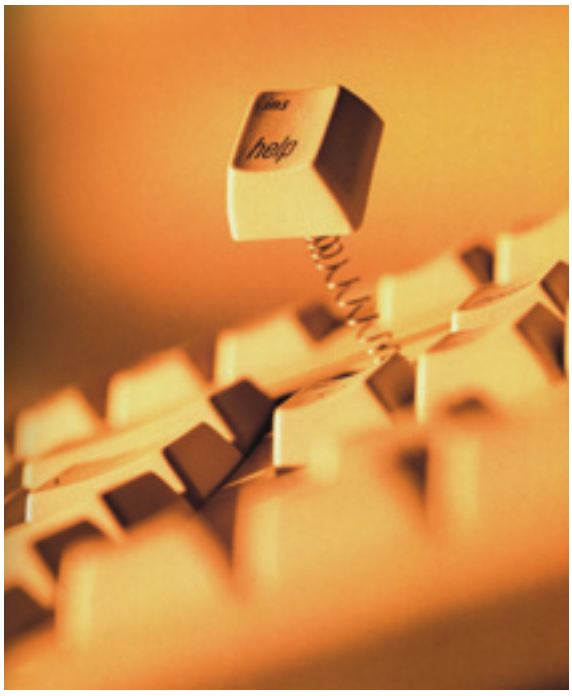


HIPAA Security

More Than Just Compliance



HIPAA Security

More Than Just Compliance

Executive Summary

Virtually all healthcare providers will need to comply with HIPAA's requirements to secure electronic patient information by April 2005. In today's interconnected virus-infected world, where technology changes almost daily, this will not be easy.

This paper examines the HIPAA Security Rule within a broad context. In it, we build the business case for compliance. Healthcare organizations need to address security not as a government mandate but as a business issue. This is a regulation whose time has come.

Protecting the confidentiality, integrity and availability of *all types* of electronic information is becoming an increasingly significant societal concern, one with substantial economic impact. In 2002, the worldwide cost of worms and viruses was estimated at $45 billion. U.S. corporations are already spending 8% to 12% of their IT budgets on security. Yet we continue to see viruses and worms like *MyDoom* and *SoBig* bring even the most sophisticated businesses to their "technological knees."

Organizations in all segments of our economy have a responsibility to take action to address growing security threats. With increasing amounts of health-related data being kept on line, healthcare providers have a special responsibility to protect the often-sensitive information they retain on their patients.

The Security Rule sets minimum expectations regarding administrative, physical and technical safeguards providers must implement. While there is considerable synergy between these regulations and those pertaining to patient privacy, implementation expectations are markedly different. The Rule is *comprehensive*, providing reasonable standards; *scalable*, accommodating providers regardless of size or resources; and *technologically neutral*, giving providers latitude to select technology tools that best address their needs.

Risk analysis is a regulatory requirement and the foundation upon which a provider's security plans are built. Actions taken to secure ePHI are expected to be appropriate to provider circumstance. In order to determine the reasonableness of these actions, providers must complete a risk analysis, establishing a benchmark for assessing compliance. Failure to conduct such an analysis as a precursor to taking action invites future problems, including spending too much and doing more than necessary.

For Information on GetHIP-Security Contact:

Randy Weisheit at 866-436-7047

Or via e-mail at info@www.hipaahomecare.com

By April 2005, virtually all healthcare providers will need to comply with HIPAA's Security Rule, the third set of regulations promulgated as a result of passage of the Health Insurance Portability and Accountability Act of 1996. Achieving compliance with the Rule's mandate to protect electronic patient information will be far more challenging than complying with the Privacy regulations and Electronic Transaction requirements that preceded it. For in today's interconnected, virus-infected world, ensuring the security of any form of electronic information is an increasingly significant challenge.

This security challenge must be tackled head on, not just as another "painful" federal mandate, but as an essential business activity. In this paper, we examine the industry dynamics behind HIPAA and review the Security Rule's requirements within the context of the security challenges facing organizations in virtually every segment of our economy. We explain, in plain English, what healthcare providers will need to do to achieve compliance.

WHY HIPAA...WHY NOW?

Passage of HIPAA was the culmination of nearly a decade's work driving toward the goal of creating a more efficient electronic environment in which to conduct the "business" of healthcare. The Act, quite frankly, has little to do with insurance portability and the need to ease the job-changing burdens associated with our increasingly mobile society. Electronic transaction, patient privacy and information security provisions were incorporated to provide impetus to increase information technology use throughout the healthcare industry.

Rather than considering HIPAA an opportunity to position their organizations for the future, however, many providers have adopted a posture that it is just another regulatory burden. Patient privacy is too often interpreted largely within a legal context as rules, financial penalties, and jail time for chronic offenders. Transaction standards have been viewed as a technical challenge for software vendors and a training challenge for medical records and billing staff. Now, the security regulations are looming.

To better understand the Security Rule's requirements it is beneficial to examine them in a much broader context. It is widely acknowledged that healthcare lags behind other sectors of our economy in its use of information technology. The industry's general reluctance to aggressively address this situation has profound implications on both the cost and quality of patient care. Facing an unprecedented challenge in just a few years as millions of aging "Baby Boomers" place increased demands on the healthcare system, the industry has little choice but to transform itself through increased use of information technology. HIPAA is one of the initial steps in this transformation, though savvy healthcare providers know they must do more with less regardless of the efficiencies realized through technology.

In his 2004 State of the Union address, President Bush became the first U.S. President to tell the nation, *"By computerizing health records, we can avoid dangerous medical mistakes, reduce costs and improve care."* Just a week earlier, New York Senator Hillary Clinton unveiled a proposal to modernize the healthcare system noting, *"In the 1990s, many industries transformed through the use of information technology. Healthcare has not done so but can and should. Information, in the hands of the right people, at the right time, drives quality and value."*

Healthcare expenditures now represent 15 percent of the nation's Gross Domestic Product and this percentage will certainly continue to rise. Significantly, the challenge *and* the solution are recognized on both sides of the political aisle.

THE NEED FOR SECURITY

What will be necessary to move forward, aside from the obvious need for an industry-wide commitment and a substantial investment of time and money? According to the Institute of Medicine's 2002 report, *Crossing the Quality Chasm*, initiatives to expand information technology use will remain stymied until the general populace has confidence that medical records stored and exchanged electronically are protected. Hearing reports almost daily about identity theft, computer hackers and viruses and worms, Americans want assurances every effort will be made to secure their medical records.

This is not an issue limited to healthcare. Protecting the confidentiality, integrity and availability of *all types* of electronic information is becoming an increasingly significant societal concern, one with a substantial economic impact. As Richard Clarke, former White House cybersecurity czar, and Lee Zeicher, *Optimize Magazine*, note in a recent article on computer security (*Security Pipeline*, January 6, 2004), the numbers tell the tale.

- ✔ In 2000, there were 21,000 reported virus incidents. Three years later, the number was more than six times higher.
- ✔ In 2002, the worldwide cost of worms and viruses was estimated at $45 billion; August 2003 alone saw costs of almost the same magnitude, while the annual cost will rise 300% year over year.
- ✔ Twenty-seven million Americans have been the victims of identity theft in the past five years, but one-third of that total were victimized in the past 12 months.
- ✔ Patches to correct the kind of commercial-software vulnerabilities that hackers target most frequently were once issued at a rate of maybe 10 per month. In 2002, they appeared at a rate of dozens per week.
- ✔ And in 2003, worms that used to take several days to travel around the globe spread to more than 300,000 systems on six continents in less than 15 minutes from launch.

The public's security concerns are well-founded. As Clarke and Zeicher point out, the implications for corporate America are huge. *"Five years ago, U.S. corporations spent 2% to 3% of their IT budgets on security; now that portion is roughly 8% to 12%. And the worst is, it hasn't helped. In recent months, even the most security-aware companies have been victimized."*

Organizations in all segments of our economy have a responsibility to take action to address these growing threats. With increasing amounts of health-related data being kept on line, healthcare providers have a special responsibility to protect the often-sensitive information they retain on their patients. Yet how many providers can say they are truly fulfilling this responsibility?

SECURITY IS DIFFERENT

Protecting the confidentiality, integrity and availability of electronic protected health information (ePHI) is the focus of HIPAA's Security Rule. The regulations set forth minimum expectations regarding the administrative, physical and technical safeguards that providers must implement to secure ePHI. It is the first time such national standards have been specified for healthcare providers, and its requirements are based on sound, time-tested security approaches. It is a regulation whose time has come – it makes good business sense.

While there is considerable synergy between HIPAA regulations governing privacy and security, their respective implementation expectations are markedly different. Where the Privacy Rule is highly *prescriptive*, addressing specific patient rights and requiring implementation of a broad set of administrative policies and procedures, the Security Rule provides considerable *latitude* regarding the manner in which healthcare organizations achieve its goals. Providers will need to evaluate the merits of various security tools and approaches in determining which will best address the Security Rule's requirements in light of their particular organization's needs.

Unlike the Privacy Rule, providers must perform a risk analysis and formulate a risk management plan to address any "gaps" that have been identified. Security solutions deployed will need to be provider-specific taking into account an organization's operations, environment and technology resources. This will present a particular challenge to multi-site providers who may have addressed Privacy Rule requirements by developing and mandating a corporate set of policies and procedures, forms and training materials for use in all locations and settings. Much of the effort required to address security requirements will have to be performed on a site-specific basis as risks may vary significantly from location to location and setting to setting.

The Security Rule also places much greater emphasis on continuously monitoring both operational and environmental changes. Periodic review and revision of security practices are required to reflect such changes. Compliance is not a one-time achievement. With new technological threats emerging almost daily a system considered secure today will not necessarily be secure 6 months from now. The need to remain vigilant regarding security is obvious.

FRAMEWORK FOR IMPLEMENTATION

It took more than four years following publication of the draft HIPAA security standards in 1998 to prepare the final Security Rule. During that time, security objectives were refined and key principles guiding development of the final requirements better-defined in light of provider comments.

The Security Rule requires providers to ensure that the confidentiality, integrity and availability of ePHI are adequately protected. Within the context of the final rule these are defined as follows:

✔ **Confidentiality:** Access to ePHI is limited to authorized individuals or entities, and such authorization is consistent with necessary use and disclosure provisions governing privacy.

✔ **Integrity:** Patient data stored (at rest) in a provider's information systems and ePHI exchanged with other entities (in transit) must be protected from unauthorized modification or manipulation.

✔ **Availability:** ePHI must be available to authorized individuals or entities when it is needed and steps must be taken to ensure this data is not deleted or destroyed while at rest or in transit.

In order to specify standards that could be applied to the broadest possible audience, the security regulations were formulated based on three guiding principles.

✔ **Comprehensiveness:** Requirements are *comprehensive*, providing a reasonable set of standards for protecting the confidentiality, integrity and availability of ePHI. At the same time, it is acknowledged that no solution can guarantee security.

✔ **Scalability:** Recognizing the diversity of healthcare organizations, the regulations are *scalable*. They are sufficiently flexible to accommodate providers regardless of size or resources.

✔ **Neutrality:** The regulations also recognize the rapid pace of technological change and thus are *technology neutral*. Providers can select the technology tools necessary to best address their specific security needs.

SCOPE OF THE SAFEGUARDS

Security is much more than making certain computer systems are protected against hackers or that applications in which ePHI is found are password-protected. The Security Rule recognizes this and requires providers to create an environment in which reasonable administrative, physical and technical safeguards are in place to protect the confidentiality, integrity and availability of ePHI.

Understanding the scope of safeguards encompassed by the Security Rule is crucial to achieving compliance. It is also a prerequisite to implementing appropriate controls. For, achieving security in one particular domain does not necessarily accomplish the ultimate goal, providing patients adequate assurance that all necessary steps are being taken to protect their health information.

To accommodate the diverse environments in which safeguards must be implemented, the Security Rule incorporates a novel approach including both *required* and *addressable* specifications. Providers are expected to evaluate security standards and implementation specifications to determine how they can best be addressed. They are even given the option to decide that an addressable implementation specification is simply not applicable.

✔ **Administrative Safeguards:** These are the policies and procedures, risk management processes and other administrative actions taken to ensure ePHI is adequately secured, including designation of a security official and staff training. They encompass 22 implementation specifications, 12 of which are required and 10 that are addressable.

✔ **Physical Safeguards:** These include the security measures put in place to control access to and use of a provider's facilities, workstations and electronic media. There are eight implementation specifications, two of which are required and six that are addressable.

✔ **Technical Safeguards:** These are the technology-based safeguards implemented primarily to monitor and control electronic access to ePHI, including such items as firewalls, virus protection and encryption software. There are nine implementation specifications, four of which are required and five that are addressable.

As noted, the Security Rule's requirements represent a baseline standard for securing ePHI. The chart at the end of this document presents a summary of the safeguards that providers must consider as they develop their risk management plans and implement controls necessary to ensure confidentiality, integrity and availability are adequately protected.

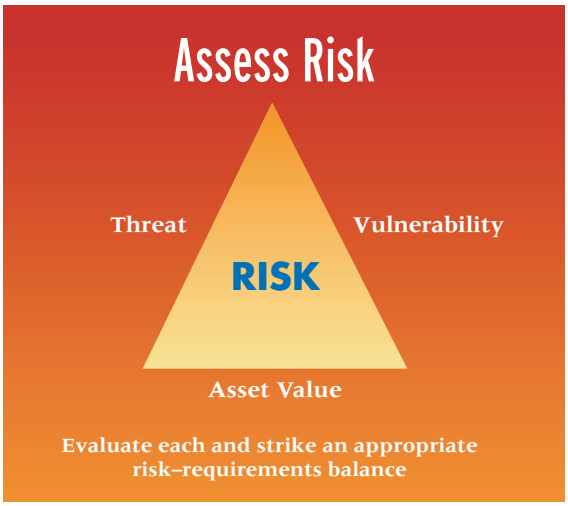
RISK ANALYSIS IS ESSENTIAL

Risk analysis is the foundation upon which a provider's response to security requirements is built. In summary, providers must examine how ePHI is used in their day-to-day operations. They must review all relevant policies and procedures and must document where ePHI is stored, how it is accessed and how it moves throughout their organization. Existing controls need to be identified as do potential security vulnerabilities. A risk management plan must be formulated to address any shortcomings, and any actions ultimately taken to address "gaps" must be documented. Finally, providers must monitor on-going performance to ensure ePHI is not compromised by future operational, environmental or technological changes.

HIPAA regulations assume actions taken to secure ePHI are appropriate to provider circumstance. This is where scalability and platform neutrality enter the picture. Actions are expected to be taken that would be considered reasonable in light of organization size and information technology use. To ultimately determine whether security measures put in place are reasonable, a baseline assessment must be performed. Without this benchmark, providers have no basis on which to defend their actions.

Risk is determined by three factors: *asset value*, *threat* and *vulnerability*. The model illustrated below is widely used in the insurance industry to define risk. Our discussion is adapted from a paper presented by Peter J. Haigh at the 2001 HIMSS annual meeting.

In this model, risk equals the area of the triangle. For those readers who recall their basic geometry, reducing the length of any one of the sides results in a proportionate reduction in the triangle's area (risk). Using Haigh's metaphor, if an open window represents a vulnerability, then closing it reduces risk and putting a lock on it reduces risk further.



To illustrate the application of this model to risk analysis and risk management, let's contrast a situation encountered at a typical hospital nursing station with one that might be found in any small provider's office.

In the hospital setting, clinicians can access virtually all patient data from workstations located on each floor. Typically, they log in at the beginning of a shift and log out at the end. Multiple clinicians are likely to share a workstation. All of this takes place as friends and family walk by to visit patients. In this situation, asset value (all clinical data), threat (public traffic) and vulnerability (log on/off, multiple users) are all high – risk is substantial. As a result, many hospitals are considering use of biometrics (e.g. fingerprints, retinal scanning) as a means to control access, decreasing risk by reducing the vulnerability side of the triangle.

Now consider a typical small provider office where a staff person is scheduling appointments. This individual may be working in an area where there is little or no public traffic. They are the only person who uses their workstation during the course of the day and they may have access to only a portion of the patient's record. In this example, all sides of the triangle are small. The area inside the triangle is substantially less than in the hospital example, thus risk is low. An appropriate and reasonable (and we might add much less costly) solution in this situation might be guidelines requiring that passwords be changed once per month.

In order to arrive at a judgment regarding the reasonableness of solutions in either of these situations, all three sides of the triangle need to be examined but not all need to be adjusted in order to achieve the goal of risk reduction. This is the essence of risk analysis. Failing to conduct such an assessment as a precursor to taking action invites future problems, including spending too much and doing more than is necessary.

ADMINISTRATIVE SAFEGUARDS	
Security Management Processes	❑ Examine risks to ePHI captured, retained and transmitted; identifying potential vulnerabilities to the confidentiality, integrity and availability of ePHI. ❑ Utilizing risk analysis results, implement reasonable and appropriate security measures to reduce risks and vulnerabilities and to achieve compliance. ❑ Implement sanctions to be applied to all workforce members that violate security policies and procedures. ❑ Implement ongoing security monitoring efforts, including procedures to monitor system activity.
Security Responsibility	❑ Designate a single individual to serve as the security official (analogous to the privacy official position, these positions may be combined).
Workforce Security	❑ Ensure workforce members have appropriate access to ePHI and implement policies and procedures as needed to limit or prevent access to ePHI when such access is not necessary.
Access Management:	❑ Manage the process for authorizing workforce member access to ePHI and implement policies and procedures to ensure appropriate access (authorizations consistent with minimum necessary use determinations).
Security Awareness and Training	❑ Provide security training to workforce members and implement an ongoing security awareness program (training prior to the compliance deadline).
Security Incidents	❑ Implement policies and procedures to identify and respond to suspected or known security incidents and to mitigate the harmful effects of such incidents.
Contingency Plan	❑ Evaluate the criticality of software applications and files containing ePHI. ❑ Develop a contingency plan including policies and procedures for responding to emergencies or other events that could damage systems containing ePHI. ❑ Implement, procedures to restore any data lost as a result of a natural disaster. ❑ Implement procedures to protect the security of ePHI while operating in an emergency mode. ❑ Determine how contingency plans will be periodically tested and revised.
Evaluation	❑ Periodically evaluate security safeguards to demonstrate and document compliance with internal security-related policies and requirements.
Business Associates	❑ Identify business associates and obtain satisfactory assurances that they will appropriately safeguard ePHI (in place by the compliance deadline).
PHYSICAL SAFEGUARDS	
Facility Access Controls	❑ Implement policies and procedures limiting physical access to information systems and facilities.
Workstation Use	❑ Implement policies and procedures addressing acceptable workstation use (includes terminals, desktop computers and portable devices).
Workstation Security	❑ Implement safeguards limiting access to workstations to authorized users and securing the devices themselves.
Device and Media Controls	❑ Implement policies and procedures addressing disposal of computing equipment and electronic media that contain ePHI. ❑ Implement policies and procedures addressing re-use of electronic media that contains ePHI. ❑ Determine how records regarding equipment movement and disposal will be maintained. ❑ Identify backup activities to be performed when computer equipment is moved or replaced.

TECHNICAL SAFEGUARDS	
Access Control	❑ Implement technical policies and procedures regarding assignment of unique user IDs to individuals authorized to access ePHI. ❑ Establish procedures controlling access to information systems during emergency situations, when individuals not routinely authorized to access ePHI may need to do so. ❑ Determine if automated procedures terminating a system session after a predetermined time period are needed. ❑ Determine if encryption of ePHI stored in information systems is warranted.
Integrity	❑ Determine appropriate mechanisms to protect the integrity of ePHI (implementation will be determined based on operations, environment and controls already incorporated in software applications).
Person or Entity Authentication	❑ Implement procedures to ensure that the identity of any person or entity seeking access to ePHI is verified.
Transmission Security	❑ Implement technical security measures, as necessary, to ensure that ePHI is not accessed by unauthorized individuals while it is being transmitted over a network.

About The HIPAA Implementation Program

The HIPAA Implementation Program (HIP) has been developed by Stony Hill Management, home care's leading technology consultants. Hundreds of healthcare organizations across the country utilized *GetHIP-Privacy* to comply with Privacy Rule requirements. Now we are offering *GetHIP-Security*, addressing HIPAA mandates to secure electronic health information. This latest software release utilizes the same easy-to-use TurboTax®-like interface we built into *GetHIP-Privacy* and explains every aspect of the Security Rule in plain English.

GETHIP-SECURITY - HOME CARE'S #1 CHOICE

Since its introduction in fall 2004, *GetHIP-Security* has quickly become the home care industry's number one choice for complying with the HIPAA Security Rule. Our software is used at more than 1,000 locations throughout the U.S. It has been endorsed by more than 25 state and national trade associations and is recommended by numerous software vendors. Dozens of leading home care companies have chosen *GetHIP-Security* as their HIPAA compliance solution. Both single-site and enterprise software versions are available, with prices starting under $1,000.

STONY HILL MANAGEMENT

Established in 1994, Stony Hill Management is an educational resources and consulting company serving healthcare providers throughout the U.S. Our focus is on non-acute healthcare settings and we are widely regarded as home care's leading technology consulting company. We offer a variety of technology-related publications and have conducted hundreds of educational seminars for healthcare provider groups across the country. Stony Hill Management is a privately held company located in Fredonia, Wisconsin.

Stony HILL MANAGEMENT, INC.

For Information on GetHIP-Security Contact:
Randy Weisheit at 866-436-7047
Or via e-mail at info@www.hipaahomecare.com