InformationWeek
:: analytics
InformationWeekanalytics.com

February 27, 2009

Analytics Alerts

HIPAA: Time To Get Serious

Contents

The Feds are coming. Don't believe us? In July 2008, the Department of Health and Human Services fined Providence Health System $100,000 for security lapses, and the department has contracted with Pricewaterhouse Coopers to conduct additional audits. As of January, HHS had issued 47 corrective action plans. With the imminent appointment of a new HHS director, we don't expect this pace of enforcement to slack off. Are you at risk?

Confused About HIPAA? Follow Our 10 Step Program To Get Serious About Compliance

By Avi Baumstein

We expect to see the Centers for Medicare and Medicaid Services—the unit within the Department of Health and Human Services responsible for HIPAA compliance—place greater emphasis on proactive enforcement in the coming year. The impetus? A report issued in October by the HHS Inspector General faulting CMS for not providing effective oversight and enforcement of HIPAA security. We're also watching closely the pending appointment of a cabinet secretary for HHS and the Obama administration's plan to update the nation's electronic medical records system.

If you work in the health care field, you're aware that HIPAA places certain requirements on covered entities. But after that, the details tend to get fuzzy. HIPAA doesn't specify any particular technologies, there is no product you can buy that will magically make you compliant, and there's no sanctioned checklist or certification to guide you. This is, to an extent, by design: One goal of HIPAA was to be a one-size-fits-all, technology-neutral regulation.

Many infosec pros enjoy this flexibility; some wish for more guidelines. Whatever your stance, HIPAA requires that IT tailor a security program to its specific environment. To help, we combed through the regulations, searched out clues as to what CMS is expecting, and studied HIPAA implementations to come up with 10 steps that should put you well on your way to building a security program that will pass muster, just in case the feds come knocking.

1 | Assign a security official

Sounds basic, and most large organizations have designated an information security officer. But smaller shops may not recognize the value of having a single person responsible for coordinating all HIPAA security activities. This doesn't mean the security official does all the work; rather, this is the person who will track compliance requirements and bring projects to the internal groups responsible for implementation, or identify opportunities for outsourcing.

There are several schools of thought regarding the ideal background for the security official. HIPAA specifies both a Privacy Rule (Standards for Privacy of Individually Identifiable Health Information) and a Security Rule. Many organizations chose a HIPAA privacy officer with a legal background, due to the complexity of the HIPAA Privacy Rule, and liabilities and penalties related to privacy regulations. However, the Security Rule is much more straightforward, and liability concerns are more about failing to implement security countermeasures than ensuring appropriate interactions with patients and properly documenting and reporting incidents. In this case, someone with a strong security management background is a better choice.

2 | Determine your individual risks

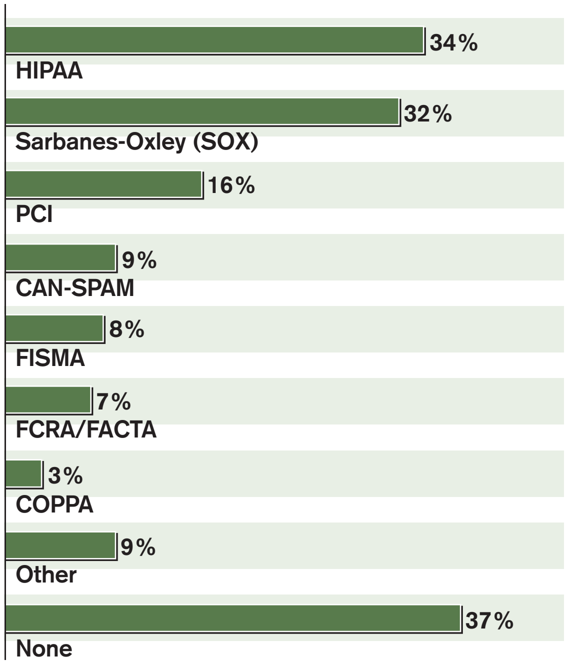
The essence of HIPAA is establishing a sustainable security management process to reduce risks and vulnerabilities to a reasonable level. This process consists of assessing risk, mitigating identified risks, and documenting risk management processes and procedures. It all starts with a risk assessment, which must be conducted at least every five years.

The first step in assessing risk is to inventory all protected health information (PHI) and systems that store PHI, a process that organizations with strong information management processes will have a leg up on. Next is determining threats to this data.

Sure, you need to protect against the sinister plots of outside attackers breaching the firewall and compromising patient databases, but you also must include more mundane threats, such as staff accessing the records of celebrity patients, theft of a device containing PHI, or natural disasters destroying a data center. It’s important at this stage to list

Regulation Compliance

With which of the following regulations is your organization required to comply?



Note: Multiple responses allowed

Data: *InformationWeek Analytics* 2008 Strategic Security Study of 1,097 business technology professionals all possible threats, no matter how slim you consider the likelihood to be, and assign probabilities to each.

There are two schools of thought when it comes to risk assessments. Some people try to get very scientific and assign numerical scores to threats and peg dollar figures to estimated losses, calculating precise-looking risk values. This metric can be useful, especially when you have a large number of risks that are close in priority. The problem, however, is that this process is really valid only if you have accurate numbers to feed into the equation. Once you start assigning threat probabilities and loss estimates according to gut feelings, precision goes out the window.

An equally valid method of calculating risk is to use values: high, medium, low, and negligible. While seemingly less precise, this method can help prioritize risks much more quickly while still providing a useful tool to determine where to allocate mitigation resources.

Your risk assessment will be used to guide nearly all of your other implementation steps. But, remember that any risk assessment is a snapshot of a point in time, and computing environments are constantly changing. This is why the concept of a security management process is so important. Every time a new system comes online, or a change to an existing system is proposed, the risks of this system or change need to be assessed. It's at this point that you can decide whether the risk is acceptable, can be transferred using insurance or some other strategy, or needs to be mitigated.

3 | Document Everything

Government security requirements are big on documentation, and HIPAA is no exception. The need for documented policies and standards comes up again and again in the Security Rule. CMS provides a list of sample questions for HIPAA security audits; most involve review of documentation, starting with policies and procedures (see www.cms.hhs.gov/SecurityStandard).

What needs to be included in your policies and procedures? The HIPAA rule says only that rules have to be reasonable and appropriate to comply with the regulation. This is pretty vague, but a good place to start is with the standards in the security rule. This introduces a key concept in HIPAA: Standards are either “required” or “addressable.” Obviously, required standards have to be implemented, although most of them still provide enough room to customize to your environment. Addressable standards are interesting because they can be met by deciding (and documenting) that a standard isn't applicable or a concern in your environment, or that you've addressed the standard in some alternative manner.

The Security Rule comprises three sections: Administrative, Physical, and Technical safeguards. These would make handy divisions for your policy set. Administrative safeguards include assigning a security officer, having policies and procedures, conducting risk assessments, and having contingency plans. Physical safeguards cover facility access controls and measures to protect the computers that process and store patient data from intrusions as well as natural disasters. Technical safeguards include standards for logging, auditing, access control, antivirus measures, encryption, and more. Your policy should cover how your organization will implement or address each of the standards, and who is responsible for that implementation.

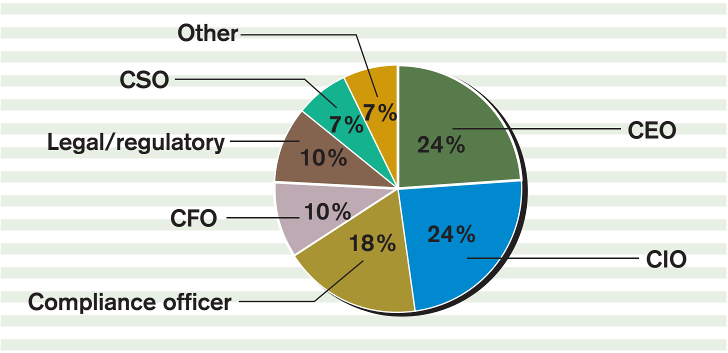
This is where you'll put the results of your risk assessment to work, ensuring that you have policies in place to address any of the significant risks that were identified.

4 | Know Your Users

CMS says that information access management and access control are the two most commonly violated provisions of the security rule. Information access management comprises your policies and procedures to authorize access to PHI. This is one place where the Security Rule specifically references the Privacy Rule, requiring that information access management policies be consistent with the provisions of the Privacy Rule, as far as who has access and under what circumstances. Key to complying with this provision is documenting these access authorizations. CMS has stated that a likely request in a compliance audit will be for a list of all users authorized to access systems that store, process, or transmit patient data. It's a sure bet that the auditor will want to look at your systems, to compare this list to who really does have access.

Primary Risk Management Driver

Who is the primary driver behind your risk management initiative?



Base: 505 companies with risk management initiatives in place

Data: *InformationWeek Analytics* 2008 Strategic Security Study of 1,097 business technology professionals

Access control, then, is the technical implementation of information access management. Once a user is authorized for access to PHI, how will she gain that access? In many organizations, it was common practice for users, especially providers moving among patients, to use a common account for access to patient systems, even leaving computers logged on for the next user. If you fell for this convenience, now is the time to stop. Every user must have a unique identifier to access patient data. Beyond that, every user must be specifically authorized to access PHI, so you'll need procedures that lay out how this authorization happens, be it a paper form that a manager signs or an electronic system.

And forget about accounts with blank passwords—while not requiring any particular method of authenticating users, the security rule does require that a system be in place to ensure people accessing the system really are who they claim to be. Your risk assessment should have helped you understand how great the threat would be of someone (inside or outside) trying to use an employee's legitimate credentials to access your data. This understanding will help guide your choice of authentication method, from simple passwords to multifactor systems or even biometrics.

Group Addresses Security And Privacy

Despite the aim of the Health Insurance Portability and Accountability Act to bolster the security and privacy of patient information, many health care providers believe more should—and can—be done. And a newly formed consortium of industry leaders plans to do something about it. A group of nine companies in the health care industry have come together to create a set of best security practices to heighten the security and privacy of electronic medical records. The Health Information Trust Alliance (HITrust; www.hitrustalliance.net) is a private, independent company that was created to establish a common security framework that should allow for more effective and secure access to and storage and exchange of personal health information.

Charter members include hospital-provider HCA; health-insurance providers Humana and Highmark; Cisco; GE Healthcare; Johnson & Johnson Health Care Systems; Philips Healthcare; and Pitney Bowes. HITrust announced that it will launch its Common Security Framework (CSF) on March 2, 2009. The HITrust CSF will be a set of tools to aid organizations that manage electronic health information in protecting their information assets and managing related risks and complexities and will comprise three components: the Information Security Implementation Manual, a Standards and Regulations Cross-Reference Matrix, and a Readiness Assessment Toolkit. *–George Hulme*

Pay special attention to how you will handle terminating the access of employees who leave or change duties within your company. There needs to be a triggering mechanism for a review of access rights, so this will involve HR. Large enterprises usually find identity management systems to be an efficient way to automate this process, triggering access termination based on personnel changes in an ERP system, while smaller offices could suffice with a checkbox on the termination form to have IT disable the employee's account.

5 | Be Prepared To Handle Incidents

HIPAA requires that procedures be in place to identify and respond to security incidents, minimize the harmful effects of incidents, and document incidents and their resolution. This sounds simple enough, but could actually encompass a lot of work, depending on the specifics of your company. Of course, your incident response needs will be driven by the risk assessment. If Internet attacks are a high risk, you may decide that complex intrusion detection systems are called for. Large companies may need to have standing incident response teams with forensics experts on staff, while smaller companies could suffice with these duties assigned to existing staff and plans to outsource specialized tasks during an incident.

No matter the size of your organization, documentation of incidents that do happen is crucial. There is no requirement that security incidents be reported, but CMS says that its trigger for enforcement will be complaints, which often result from incidents. You can be certain that should auditors show up, they'll want to see documentation of incidents, both to get the other side of a complaint and to determine whether incidents are being properly dealt with and learned from.

6 | Expect The Worst

HIPAA isn't just about protecting data from unauthorized access. As more information needed for patient treatment and billing becomes electronic, it's crucial to ensure that systems are available and the data is trustworthy. Your contingency plan must cover backup and recovery of PHI, along with preparations for recovering from disasters. Your plan also needs to include preparations for operating under emergency conditions—how business can continue without access to the electronic PHI, and how you will continue to protect data on your systems during disasters.

CMS' suggested audit questions include documentation of disaster recovery plan testing, and the results from those dry runs. Contingency planning is a huge field unto itself, and it would be very easy to get wrapped up in this step. A good strategy: Document current backup and recovery processes, and put together some basic information that would be needed to recover from a disaster. This is another good place to make use of the inventory you prepared for your risk assessment. It will provide a blueprint for what would have to be acquired if your entire facility were destroyed or rendered unusable. The inventory should have some information regarding criticality of those systems to your business, which will help in prioritizing what to replace after a disaster.

If your risk assessment turns up any glaring problems in your backup and recovery process, such as a lack of off-site storage, tackle the issues. But unless you have very significant threats that you haven't prepared for, it's probably best to come back around to more detailed contingency planning after dealing with the other steps needed for compliance. Just don't let this turn into uncontrolled procrastination.

7 | Control Your Media

The management of devices and media used to store patient information is another top source of HIPAA violations, according to CMS. The Security Rule includes four provisions covering devices and media. First, you must have policies and procedures governing the disposal or reuse of media used to store patient data. Any time a security researcher wants some quick publicity, they buy some old computers on eBay and look for confidential data left on them. They are rarely left without a story. To address this, your company needs firm procedures to ensure this can't happen. These rules could state that hard drives are removed from old PCs before they're sold or recycled, or at minimum that drives are wiped with a utility, such as Secure Erase from the University of California San Diego's Center for Magnetic Recording Research.

The same goes for other types of media, such as retired backup tapes and USB memory sticks. Likely, you already have a shredding vendor handle your paper records, and many of these vendors also handle destruction of electronic media. This is a situation where spending a little money will save a huge amount of staff time.

HIPAA also includes provisions for tracking of storage media and devices as they are moved around the facility and disposed of, as well as data backup. Both of these are addressable, because they may not be equally important to all size organizations. Small offices, for example, likely won't be buying large quantities of new computers and shuffling them around the facility, such that something may fall through the cracks. But a large hospital system will constantly be doing equipment refreshes, so mistakes could more easily happen. Data backup is covered as part of device and media controls as well as within the contingency plan requirements. Beyond the standard disaster recovery needs in the contingency plan, the backup provisions under device and media controls are intended to ensure that the only copy of valuable data isn't lost when an old computer or retired media is disposed of.

Resources:

The University of Miami's free Privacy/Data Protection Project Health Information Privacy and Security (HIPS) course series: **http://privacy.med.miami.edu/hips/index.htm**

CMS HIPAA Security Rule in pdf format: **www.cms.hhs.gov/SecurityStandard/Downloads/securityfinalrule.pdf**

8 | Train Users, Then Remind Them

Users really are crucial to security, but it's very easy for infosec pros to assume they already understand the issues. So easy, in fact, that a lack of security-awareness training is another of CMS' most common violations. All members of your workforce need ongoing security training appropriate to their jobs. HIPAA leaves it up to you to decide what is appropriate and how the training should be conducted, although the provision describes the training as "periodic security updates."

Organizations approach this training requirement in a number of ways, from posters in the work area to reminders posted on computer login screens to online training covering the security policies, or even mandatory classroom training. It's important to ensure that your training be adjusted as the environment changes—as systems are updated, or the experience of your staff increases—as well as when your threat landscape morphs. This is another case where your risk assessment will help guide your choice and provide a solid justification should you become subject to an audit.

9 | Log/Audit

HIPAA requires that covered entities record and examine activity in systems that store or use PHI. The type of high-risk threats you identified in your risk assessment will help you decide what needs to be logged in order to meet this requirement, but it's important to understand the context. The Security Rule goes to great pains to ensure that users are uniquely identified and authenticated. Oftentimes, in a medical setting, it's difficult to predict who will need to access which patient's data, and strong limits on this access could cause dangerous delays in treatment.

Instead, reasonable access restrictions should be implemented, and followed up with audits of access trails to ensure that employees are not looking at or modifying records they shouldn't.

These audits also help support the Privacy Rule requirements that providers be able to supply an accounting of every instance a particular patient's information was accessed.

10 | Clean Up Old Data

This step will greatly simplify your HIPAA compliance efforts by reducing the amount of data you need to protect. Hopefully, when you did your inventory for your risk assessment, you didn't just focus on the systems in day-to-day use, but really scoured the data closets for older gear and disused databases. Often, when a system is replaced, IT will decide to keep its predecessor as a fallback, just in case there are problems. Or, users may demand the old system be saved, almost as a security blanket. While not an unreasonable practice if well managed, all too often the old system is forgotten and left running in a dark corner, sometimes for years. These relics can pose an even greater danger than the ones in active use—even if your administrators remember they're still there and try to keep them secure, patches and updates may no longer be available.

Once you've used your inventory to identify outdated data and systems, you then need to make the classic closet-cleaner's decision: toss or keep? Your first reaction should be to purge the data, but hold off and check whether the data is required to be kept for legal (log and data retention) or business reasons. If there is a reason to keep the data, does it need to be online and accessible? If not, archive it to durable media and store it in a vault, or with an off-site data storage company. Data on a tape in a vault is not susceptible to hackers or curious employees.

What if the data can be accessed only by a particular application that is no longer in use? One option is to convert the physical system to a virtual machine. Just don't leave it spinning—back it up and place those backups in the vault. If the hardware is really unusual or outdated, you may have to keep the whole system, but be sure it is powered down and not accessible via the network.

Before placing any old data in storage, know when it can be destroyed, and make sure a process is in place to get rid of it when the time comes. A data disposition policy helps here.

Data purging is not limited to unused systems. Because disk is cheap and databases can handle such huge amounts of information so easily, every organization tends to collect data that is no longer needed. Keeping lab test results that have outlived their usefulness or records on patients who have long since moved on, beyond when you're legally required to retain them, will create an even bigger mess should a breach occur.

Here's one last piece of advice: Keep your assessment going. Because the specifications in the Security Rule are written in a very general way, it means that compliance is going to be a moving target as your organization and technology evolves. This really is a good thing, because what is considered prudent today may seem laughable in a few years.

Constantly review your security compliance program in light of internal changes, varying external threats, and the available technologies and best practices in your industry to ensure you are doing what an auditor would consider reasonable and appropriate. While far from a complete guide to HIPAA security compliance, revisiting these 10 steps regularly, and consulting with legal counsel when needed, should provide a good start to building the type of sustainable security program that HIPAA requires.

Avi Baumstein is an information security analyst at the University of Florida's Health Science Center. Write to him at abaumstein@nwc.com.

SIM Eases HIPAA Compliance

By Tim Wison, Dark Reading

Collecting millions of security incident alerts without the manpower to interpret them doesn't do much to improve security. Just ask health insurer Priority Health, whose security staffers had been drowning in alerts from the firm's firewalls, intrusion detection system (IDS), and system logs, trying to separate real threats from the false alarms.

Priority Health, which has 500,000 customers, was getting frustrated with the time-consuming and tedious process—as were its auditors. The firm, which provides health care insurance to 100 acute-care hospitals and over 12,000 doctors and other health care providers in Michigan, had to better integrate its security tools and the data it was generating. Pressure was on for HIPAA-compliance, too. "Because of emerging HIPAA reporting regulations regarding log activity, we needed to monitor the activity on our systems and network more closely than we had in the past," says Tim Maletic, information security engineer at Priority Health.

Priority Health purchased ArcSight's ESM, a security information management (SIM) product, about two years ago to provide more integration and better visibility across its security infrastructure. "We had relied on a number of individual security silos: firewall logs, IDS events, and operating system events, so there was no easy way for a security administrator to get a complete view of what was happening," says Paul Melson, information security officer at Priority Health.

And at the end of last year, the company added ArcSight's Logger, a turnkey appliance that simplifies the capture and analysis of security log data. "When the auditors show up each year, we can quickly generate reports that illustrate what was happening on our network and how we responded to suspicious activities," Maletic says.

Meanwhile, the ArcSight ESM SIM, which cost the firm about $50,000, made sense because it was able to work with various types of vulnerability data. The insurer also liked the design of ESM's central console interface and its ability to correlate different security events. Priority Health first installed ESM in a small deployment that collected information from a handful of Internet-facing systems, such as its firewalls and operating system logs, all sitting in its DMZ. That configuration alone lowered the number of incoming security incidents from millions to hundreds, and also provided the security staff with more detailed information about each of the events. "We could now take a single event and put it into context with a few clicks of the mouse," Melson says. "We no longer had technicians spending an hour or two trying to figure out whether an event was a threat or not."

Mistake Or Threat?

It's also easier to determine whether multiple password attempts, for example, are the result of a user fat-fingering or forgetting his or her password, or an attacker probing the company's network. Priority Health also integrates its Microsoft Active Directory security logs (basically anyone logging in, logging out, or changing data) to ESM, as well as system logs from the company's Unix servers and its Websense Web-filtering monitor. "Most off-the-shelf security software is unable to keep pace with rapidly changing malware," said Melson, who estimates that 30 percent to 40 percent of malware goes undetected by currently available tools.

Melson says although the health care insurer is content with ArcSight ESM's features, Priority Health would like to see the product more tightly integrate with its asset management system. "We can load information from [the asset management system] into ESM now, but the process is not as quick and seamless as we would like it to be," he says.

Meanwhile, Priority Health considers its security information management implementation a competitive edge. "Because ESM automates the evaluation of our daily security incidents, we now have more efficient security practices than our competitors, and that ability provides us with a competitive edge," Melson says.

Tim Wilson is site editor and co-founder of Dark Reading. Write to him at twilson@techweb.com.

Thumb Your Nose At HIPAA, Save $100K

By Ira Winkler, Internet Evolution

A few years ago, I was talking to a security staff member of a Boise-area health insurance organization. He was bemoaning his organization's lack of HIPAA readiness, and executive-level indifference to the issue. The CEO's rationale: They had plenty of time because the government wasn't going to come to Idaho to make an example of a small company. Instead, the CEO said he'd wait to see what the actual penalties were before spending any money on HIPAA compliance.

Sadly, that CEO was a genius.

What got me thinking about this conversation was an article about the Department of Health and Human Services fining Seattle-based Providence Health and Services $100,000 and forcing the company to make security improvements. Apparently this was the result of losing 386,000 patient records in 2005 and 2006 containing personally identifiable information on unencrypted storage media.

Think about this from a risk perspective. If you do nothing, you spend nothing. If the government decides to make you an example to others, you end up being fined $100,000 and then being forced to spend money you would have had to spend anyway to implement a security program. The $100,000 cost would be covered by insurance and offset by the fact that you saved hundreds of thousands of dollars by not spending any significant money on security.

In its most basic terms, HIPAA requires insurers and health care providers to physically and electronically secure information against unauthorized retrieval, securely store the data, and be able to access it in the event of an emergency.

And yet, the $100,000 is really the only risk, and when you look at the fact that only one health care organization has actually been penalized, it is only good business sense not to spend money to become HIPAA compliant. The odds of HHS coming after you are so minute that I am finding it hard to justify heroic efforts to comply with HIPAA.

Sadly, this is not unique to HIPAA compliance. We have seen many egregious acts and indifference on the part of retailers and banks. The FTC likes to point to a couple of cases where they fined companies and made examples of them. Like the HHS, the FTC picks and chooses the very rare cases that they want to take on. The commission is only interested in making examples out of a few very serious violators. As long as companies and health care organizations can remain under the radar, they'll continue to get away with making very little effort on security. While reporters like to refer to fines as the "teeth" of regulatory enforcement, the reality is that the teeth have to be sharp. I don't believe that fining someone, who saved millions of dollars ignoring security, puts much bite into anything.

Maybe HHS is taking baby steps, and they will toughen fines and enforcement. Hopefully, they'll start in Boise.

Ira Winkler is a former National Security Agency analyst and author of Spies Among Us.

Hospital Security Ailing, Study Says

By Tim Wilson, Dark Reading

Security consultant's warning: Hospitals can be dangerous to your personal information.

From 2006 to 2007, more than 1.5 million patients' personal information was exposed through hospitals alone, according to a study released earlier this week by research firm HIMSS Analytics and Kroll Fraud Solutions, a risk management firm. That doesn't count insurance companies, pharmaceutical companies, or individual doctors' offices.

And those are only the breaches we know about. Some 44 percent of hospitals that experienced a breach last year did not inform the patients whose records were affected, according to the study.

Hospitals are not paying enough attention to security issues, and the steps they are taking are often ineffective, the HIMSS/Kroll study says. While there is a high awareness of the security requirements described in HIPAA among hospital IT professionals, most hospitals are putting too much emphasis on compliance—and not enough on real security vulnerabilities, the study says.

This lack of attention could lead to real problems for individuals down the road, the study warns. Hospitals are often a source for birth, health, and death records that can be very valuable to criminals, and patient data breaches are among the most difficult to clean up, because compromises or changes can affect insurance eligibility or even patient safety if the data is manipulated.

Yet, despite these risks, more than 13 percent of hospitals report experiencing at least one breach in the past year, according to the HIMSS report. Identity theft was three times more likely to occur at a larger facility (more than 100 beds) than at a smaller facility (fewer than 100 beds).

And the situation is not getting better, the researchers warn: Of the hospitals that admitted experiencing a breach, 62 percent identified the source as unauthorized use of information, while 32 percent said the breach occurred due to wrongful access of paper records.

"Noticeably absent were breach sources associated with malicious intent, such as stolen computers and deliberate acts by unscrupulous employees," the report states. This suggests that while hospitals are focusing their efforts on protecting patient records from curious employees or accidental compromises, they have not built sufficient controls against intentional theft or fraud, the researchers say.

Statements about hospitals' efforts to protect patient data support the researchers' conclusions. For example, many hospitals said one of their chief strategies for defending against compromises is user education—which does little to protect against malicious intent.

"There is an over-reliance on employee education and disciplinary action as effective prevention and response techniques that do not address the incidence of malicious intent that is responsible for the industry's largest and most damaging breaches," the study says. The researchers call for a "paradigm shift" toward developing security defenses against malicious attacks as well as inappropriate access.

Tim Wilson is site editor and co-founder of Dark Reading. Write to him at twilson@techweb.com.