In an era of almost total reliance on computers and computer systems, keeping software up to date can mean the difference between smooth-running, efficient healthcare and life-threatening chaos.

Keeping software in optimal working order usually means installing to patches—updates that fix programming glitches and enhance security—keep computer systems safe from viruses and hackers.

And in terms of the HIPAA security rule, managing software patches is an important component of risk management that requires covered entities to minimize security risk to a reasonable and appropriate level.

Minimize your risk

The day-to-day difficulties from running an unpatched system are more problematic than they are dangerous: Software that does not work correctly reduces productivity, increases system downtime, and is more difficult to use.

But neglecting to patch software can pose a significant threat in the long run, says Rick Ensenbach, CISSP, CISA, CISM, senior security consultant at Shavlik Technologies. It can increase the risk that any part or all of a system will fail.

“It doesn’t matter where [problems] come from,” Ensenbach says. “The end result is that they’ll bring [your system] down.” And a system failure, especially when computer programs control anything from patient records to life-support systems, can have catastrophic repercussions for any organization.

Consider the issues that can arise from an improperly patched system:

- **Legal ramifications.** An improperly patched system can leave PHI vulnerable to hackers, disgruntled employees, or any others who could potentially use the PHI for their own gain. CMS and the Office for Civil Rights could potentially view this as a HIPAA security violation.

- **Wasted time and data.** Hackers don’t have to steal information to cause problems for your facility. They can also overload or crash systems, which can add up to valuable time lost and data damaged.

- **Loss of sensitive or confidential information.** Patients who feel that the security of their health information has been compromised often bring private litigation against the organization that allowed the breach.
PROPER PATCH MANAGEMENT (continued from p. 1)

- **Loss of revenue.** A system crash, virus infection, or hacker can impede productivity and disrupt the flow of business, causing your organization to lose money.

- **Negative public relations.** Any litigation against your organization or negative publicity surrounding a system failure can damage your public image.

**Plan for patchwork**

Organizations that rush to install every new patch without careful consideration often end up disappointed and frustrated, says Chad Boeckmann, CISSP, GSEC, a security consultant at Shavlik. Some patches crash systems; others simply bog them down without any immediate benefit.

Think about a patch system for your facility as you would a system for your home computer, Boeckmann says. “If you installed every patch that Microsoft sent out, you’d probably bury your home computer,” he says. “It’s the same situation in the organization. You have to look at each patch and ask, ‘Is this something I really need to do?’ There are probably some you can outright ignore, and there are others where you need to do something.”

Creating a plan for installing and managing software patches can make the process go smoothly, Boeckmann says. Follow these basic planning steps:

1. **Assess.** Carefully look at your computer systems and your organization’s needs. The National Institute of Standards and Technology recommends creating a patch vulnerability group (PVG), a task force within your organization to assess what patches are absolutely necessary and which vulnerabilities you can handle in other ways.

2. **Identify.** Decide which patches you absolutely need. Create a list that includes the names of the software vendors you plan to use and those that can potentially provide support or hear complaints.

3. **Deploy.** Install the patch and determine whether the system works properly. Then determine whether you addressed the vulnerability at hand. Someone with technical expertise and administrator privileges can examine the system code and recognize any changes. If no one on your staff can do this, certain software programs can scan and validate your system and any patches you’ve installed.

4. **Audit.** Check the entire system periodically, focusing on critical segments to make sure the patch does its job. You can do this weekly or monthly, but no less frequently than every quarter, Boeckmann says. Archive logs or reports and any information about why your organization didn’t install certain patches.

In light of the HIPAA security rule, those records are important, Boeckmann says. “You have a credible record, a recorded history of your systems, and how they’ve been managed and patched and not patched over the past
Responding to BA’s notification of security incident
Q. How should we respond when a business associate (BA) notifies us of a security incident at its organization?
A. When a BA notifies you of a security incident, take the following steps:

- Get a description of the incident and response, including actions the BA took or expects to take, says healthcare attorney Rebecca L. Williams. Determine whether your BA’s actions were appropriate or whether it needs to do more.
- Check state law. Some states require that you take specific action to respond to a security incident. For example, California’s Security Breach Notification Law requires organizations to notify the person—usually a patient or health plan member—affected by the incident, says healthcare and HIPAA attorney Reece Hirsch.
- Work with the BA to lessen harm and prevent reoccurrence. The HIPAA security and privacy regulations both require you to mitigate the harmful effects of security incidents you know about, regardless of whether they happen at your organization or your BA’s organization. Work with your BA to lessen the harm a security incident causes and prevent further damage.

For example, if your ePHI storage vendor tells you that your most recent backups were inadvertently destroyed, copy and send on-site backups to the vendor. If you don’t have on-site backups, make an unscheduled backup to reduce the amount of ePHI you’ll lose if your system crashes.

- Terminate contract if necessary. If you’re not satisfied with your BA’s response to the incident, terminate the contract, especially if your BA isn’t willing to work to lessen or prevent future harm.

Insider sources
Rebecca L. Williams, RN, JD, Davis Wright Tremaine LLP, 2600 Century Sq., 1501 4th Ave., Seattle, WA 98101-1688; 206/629-7768; becky williams@dwt.com.

Put patches to the test
Most software programs can suit both small and large organizations, but when it comes to patch management, smaller organizations may have a trickier task ahead of them.

Large health systems with sizable IT departments to analyze and manage system changes can often run patches in an isolated test environment.

They can see affects—both positive and negative—before any kind of official roll out. Smaller organizations must be more creative.

Ensenbach recommends that smaller organizations do the following:

- Back up the entire system before implementing any patches.
- Schedule system downtime in a way that minimizes any disruption to the flow of business.
- Minimize the risk of viruses and other attacks by disconnecting the entire system from the Internet, if possible.
- Install the patch and run any programs affected by it. If the patch works properly, bring the system back online.
- Monitor the system for 24 hours (or longer if it suits the organization’s needs). Software programs used less frequently may go unneeded until days or even weeks after you install a patch.

- Notify key members of the organization that you have installed the patch, and instruct staff to report any problems immediately to a system administrator.

Don’t rush headlong into the process without careful consideration. After all, that patch is an important line of defense.

“By patching a system, you’re protecting that system,” Ensenbach says. “You’re protecting it against alteration, disruption, and destruction.”
Security best practice: Use smart cards to improve medical care, comply with HIPAA

Passwords written on sticky notes, shared passwords, and work stations that remain logged on all day present major security risks. Many facilities require users to remember dozens of passwords—inevitably leading users to write them down, choose the same password for each system, or make them easy to figure out.

With the April 2005 security rule deadline looming, healthcare professionals, specifically those in IT, have expressed increased interest in smart cards, credit card-sized plastic cards with an embedded computer chip that links to user identification, according to Randy Vanderhoof, executive director for Smart Card Alliance.

“We have seen an increase in the past 18 months as the healthcare market started to look at smart cards more closely,” Vanderhoof says. “The movement is driven by the IT professionals within the healthcare sector who struggle with upgrading computers and networks in an attempt to maximize efficiency while reconciling that demand with increasing regulatory control.”

HIPAA’s language doesn’t specify how facilities can use smart cards to comply with the rule, but smart cards can track individual user access—a component into which HIPAA delves deeply.

Smart card vendors promise a HIPAA-compliant, portable solution for physicians and nurses capable of immediate access to multiple health information systems.

“Although using smart cards and technology can help ensure compliance, just the act of using smart cards does not guarantee compliance,” says Rebecca Herold, CISSP, CISM, CISA, FLMI, information privacy, security, and compliance consultant. Facilities must still combine procedures and policies with security measures.

Ins and outs of smart cards
A smart card essentially stores the identity of the card carrier. The user inserts the card into a reader at a workstation and enters a personal identification number (PIN) to access applications to which he or she has authorization.

Because the smart card doubles as an ID badge, the user carries it at all times. When the user removes the card from the reader, the reader automatically logs out the user. It’s a lock and key system; the key must be in the lock to access the info.

It can be ineffective to have personnel fumbling around with usernames and passwords, logging in and out each time they move from patient to patient or room to room. Medical staff with access to secure PHI can insert their card, verify identification with their PIN, and log out by removing their card.

One medical center’s experience
Denver Health Medical Center in Colorado decided to implement smart cards to enhance its move to electronic provider order entry in outpatient areas. “We wanted to provide a methodology for quick access and single sign-on for doctors and providers,” says Jeff Pelot, chief technology officer.

Prior to 2002, the information technology department hadn’t been overly concerned with secure network log-ins. A nurse practitioner would make the rounds and sign on to all of the PCs so a doctor could immediately access a needed application.

“Now we are trying to get to the point of instantaneous access,” Pelot says. “A smart card, with a single sign-on effort, gets us relatively close to instant and compliant access.”

“In 2002, when we were looking at this, it cost about $100 per PC to get somebody a smart card,” he says. Denver Health looked to expand smart card use, $100 dollars per user wasn’t in the budget and Pelot and his team started looking at other options.

The result? Pelot eliminated middleware—connectivity software that allows numerous processes running on multiple machines to communicate across a network—the piece that makes the smart card work and costs the most. He took a generic card not preprogrammed to work with another vendor’s middleware, and configured it to work with Windows 2000. Denver Health eliminated the need to pay for middleware because the hospital already uses Microsoft Windows. The facility pays $8 per card and $10 per license per user.

Insider source
Jeff Pelot, chief technology officer, Denver Health Medical Center, 777 Bannock Street, Denver, CO 80204-4507; 303/436-6000.
Smart cards eliminate the need for staff to remember multiple passwords and reduce the number of password requests the IT department receives, according to Vanderhoof. The cards also handle the following functions:

- Data transmission
- Protection of data access
- Memory management

The information passes from the card to the computer through an interface or a user device. Some readers plug into the computer’s serial port or USB connection. Windows 2000 and Windows XP recognize smart cards as a “plug-and-play,” like any other external drive, for example, a keyboard or mouse. Some computers today have built-in smart-card readers.

**Improved information security**

Smart cards make information access easy for users while enforcing security measures to strengthen HIPAA compliance, Vanderhoof says. They secure information and the identity of the user who has the card.

“The smart card system is more secure because it’s not just something you know [like a password], it’s something you have and something you know,” Vanderhoof says. “It’s simple security best practice.” Herold agrees that smart cards are more secure than IDs and passwords, but specifies that the best practice is the use of two-factor authentication—not the smart card itself.

Herold also agrees that smart cards can “substantially improve security.” Even if someone knows your password, he or she cannot pretend to be you without your card. And if he or she physically has the card without knowing the PIN, the system will deny access, Vanderhoof says. This combination makes smart cards extremely secure.

However, no one technology can guarantee regulatory compliance, let alone HIPAA compliance, Herold says. You still must train your users to use smart cards—and understand that they cannot, under any circumstances, share their card and PIN.

“There are no guarantees in security technologies,” she says. “People are the weakest link, and even the best technology cannot guarantee HIPAA compliance without paying diligent attention to the human factor.”

**Evaluate cost, make smart card work for you**

To run a smart card system, you need smart cards, a reader, and a computer.

A smart card itself can cost as little as a $1 or as much as $8 per card depending on memory, sophistication, and number of applications. The cost of the reader device that plugs into the computer ranges from $20–$100 dollars, contingent on quantity and requirements. Vanderhoof warns that costs can vary significantly depending on which vendor you choose and who completes the installation and setup.

You also need to consider the actual cost of creating the cards—printing the badges and photos, and updating and upgrading the computer system—software, and applications. Because each card is a computer, each card is purchased from the vendor with a licensing agreement, similar to a software licensing agreement.

Standards continue to change, and with changing standards comes improved capabilities for cards and readers. Interoperability and compatibility are at the forefront of the movement to improve healthcare.

**Implementation timeline**

Follow this eight-step timeline when implementing smart cards at your facility:

1. **Select a team.** Choose members who understand and are familiar with smart cards and HIPAA rules.
2. **Establish project objectives.** For example, consider objectives such as ensuring the confidentiality of highly sensitive medical data while improving processing time and accuracy.
3. **Decide whether to buy a smart card system or design your own.** Consider cost and the level of specialization you need the system to support.
4. **Design your smart card.** Choose the specifications, silicon provider, chip type and size, durability, reliability, etc.
5. **Choose the reader.**
6. **Design the data center.**
7. **Enroll cardholders.**
8. **Produce and issue cards, and test pilot the program.**

Time to beef-up BA agreements

Both privacy and security regulations require agreements between covered entities and business associates (BA) but each requires the agreement to include different pieces.

As of April 20, 2005, your BA agreements must meet the requirements of both. And that could mean a review and possible update of the agreement you currently use.

“To some degree, I think there’s a feeling of complacency in thinking that the BA agreements were completed when organizations responded to the [original] privacy rule,” says Rick Ensenbach, CISSP, CISA, CISM, senior security consultant with Shavlik Technologies.

The privacy regulations affect PHI in any form; the objective of the security rule is to safeguard the confidentiality, integrity, and availability of PHI that is electronically stored, maintained, or transmitted.

“Compliance is different for each organization and no single strategy will serve all covered entities,” says Brad Peska, CISSP, official with the Office of HIPAA Standards.

Update your agreement

Your HIPAA security committee or information system officer (ISO) should review and update your BA agreement to specifically address electronic PHI (ePHI) to comply with the 2005 deadline. Small health plans have until April 20, 2006.

“When most BA agreements were written, the security rule wasn’t final, so those agreements were written with only privacy and general protection of PHI in mind,” Ensenbach says. “These new changes are specifically directed at the BA’s security program and ePHI.”

“There is nothing worse than creating something as important as a BA agreement in a vacuum,” he says. “To do so only sets you up for failure. Everyone who the agreement or the addendum impacts must be kept informed of changes.”

Communication is essential, agrees Sue Dill, RN, MSN, JD, of Memorial Hospital of Union County (OH). “We have trained all our managers on our BA contract policy. We want them to use contract because we know it contains all the sections required by law.”

Pieces of the addendum

In most cases, you can continue using your existing BA agreement as long as you attach an addendum (see the sample on p. 7). Creating an addendum is more efficient than writing an entirely new agreement to address aspects the security rule requires, Dill says.

Many ISO scan the HIPAA regs for details and guidance on what to put into the addendum. Dill suggests including the following:

Definition of ePHI.

Electronic information is what you store on computers (hard drives) and on any removable/transportable digital memory medium such as magnetic tape or disks, optical disks, or digital memory cards.

This also includes media transmissions through the Internet, extranet, leased lines, dial-up lines, and private networks, and the physical movement of removable or transportable electronic storage media. Facsimiles and telephone voicemails do not count as ePHI because the information didn’t exist in electronic format prior to transmission.

Business associate duties and responsibilities.

The agreement needs to state that a BA will implement administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of your ePHI. Include that the agreement extends to the BA’s subcontractors as well.

Reporting procedures.

Clearly state the necessity to report any security incidents and the procedure to deliver that information to you promptly.

Although not required, Ensenbach suggests building an even greater level of assurance into the BA duties clause by requiring BAs to provide you copies of all security audits or assessments, regardless of whether those audits are conducted by a third party or self-imposed.

Updating your BA contracts to include the new requirements is vital to complying with the HIPAA regulations. However, these agreements shouldn’t be viewed as the last step in compliance, Peska cautions.

“Compliance is not a one-time goal, it must be maintained,” he says. “By performing a periodic technical and nontechnical evaluation, a covered entity will be able to address initial standards implementation and future environmental or operational changes affecting the security of ePHI.”

Visit www.hhs.gov/ocr/hipaa/contractprov.html to view a sample business associate agreement.

Insider sources

Sue Dill, RN, MSN, JD, VP of Legal Services, Memorial Hospital of Union County, 500 London Ave., Marysville, OH 43040.


Brad Peska, CISSP, Office of HIPAA Standards, CMS, Health and Human Services, 200 Independence Ave., S.W., Room 647-D, Washington, DC 20201.
THIS ADDENDUM TO THE BUSINESS ASSOCIATE CONTRACT ("BA Contract") is by and between you, the client, vendor, or covered entity identified as the “Business Associate” and us, Memorial Hospital of Union County, herein after referred to as “MHUC.”

WHEREAS, the Department of Health and Human Services published a final rule relating to the Security Standards under HIPAA codified at 45 CFR Parts 160 and 164 (Security Rule); and

WHEREAS, the Security Rule requires Client to ensure that Business Associate agrees to certain safeguards and terms relating to the security of Electronic Protected Health Information. Specifically, a covered entity like MHUC, in accordance with Sec. 164.306, may permit a business associate to create, receive, maintain, or transmit EPHI on the covered entity’s behalf only if the covered entity obtains satisfactory assurances, in accordance with Sec. 164.314(a) that the business associate appropriately safeguard the information.

Business associates with a current signed BA Contract, prior to April 20, 2005, have the option of signing a new BA Contract that has these provisions included or this amendment to the existing BA Contract.

NOW, THEREFORE, in consideration of the mutual covenants and agreements herein contained, the parties agree to the following:

1. The BA Contract executed by the parties is amended to add the terms and conditions in this Addendum.

2. Terms used, but not otherwise defined, in this Addendum shall have the same meaning as those terms in the Security Rule. These include but are not limited to:

   a. **Electronic media** has the meaning in 45 CFR § 160.103, which is:
      a. Electronic storage media including memory devices in computers (hard drives) and any removable or transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or
      b. Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and via telephone, are not considered transmissions via electronic media because the information did not exist in electronic form before the transmission.

   b. **Electronic Protected Health Information or “EPHI”** has the meaning in 45 CFR § 160.103, and is defined as that received from, or created or received on behalf of MHUC.

   c. **Security Incident** has the meaning in 45 CFR § 164.304, which is the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations.

3. The Business Associate will:

   a. Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the EPHI that it creates, receives, maintains, or transmits on behalf of the Covered Entity;

   b. Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it;

   c. Beginning on April 20, 2005, report to MHUC any Security Incident of which it becomes aware, in the following time and manner:

      (i) Any actual, successful Security Incident will be reported to MHUC in writing, within five (5) business days of the date on which Business Associate becomes aware of such Security Incident

      (ii) Any attempted, unsuccessful Security Incident of which Business Associate becomes aware, will be reported to MHUC in writing, on a reasonable basis, at the written request of Covered Entity. If the Security Rule is amended to remove the requirement to report unsuccessful attempts at unauthorized access, this subsection (ii) shall no longer apply as of the effective date of the amendment of the Security Rule.

2. This Addendum will be effective on the date last signed below and will terminate concurrently with the BA Contract.

3. This Addendum shall be deemed incorporated into the BA Contract, and all terms of the BA Contract shall apply. In the event that the terms of this Addendum and the terms of the BA Contract conflict, the terms of this Addendum shall control.

Source: Sue Dill, Memorial Hospital of Union County (OH). Reprinted with permission.
Incorporate HIPAA physical safeguards when renovating or relocating

If you plan to renovate or relocate your facility, consider ways to incorporate into your new layout and design the physical safeguards set out in the HIPAA regulations, says Saira N. Haque, director of corporate and HIPAA compliance for St. Joseph’s Hospital.

HIPAA doesn’t require covered entities to make structural changes to their facilities to comply. But if you are planning future physical changes, consider it an opportunity to enhance privacy at your organization, she suggests.

Haque suggests getting your privacy officer involved in the master planning process because addressing privacy throughout the renovation process saves you time and money. Also, your program can benefit from the ideas and experiences of those involved in all areas of your organization.

Don’t include OCR contact info in NPP

Don’t include a mailing address, Web site address, or phone number for the Office for Civil Rights (OCR) in your organization’s notice of privacy practices (NPP), advises New Jersey healthcare attorney Marc D. Goldstone.

The HIPAA privacy regulation requires you to include a statement in your NPP telling individuals that they have the right to complain to both you and the OCR if they believe their privacy rights have been violated. But there’s no requirement that you include the OCR’s address or similar contact information, Goldstone stays. There may be advantages to leaving this information out, he notes.

In your NPP, provide instructions to contact your privacy officer for more information on filing a complaint, he suggests. This approach meets the HIPAA requirement and gives your organization an important opportunity to speak with the individual and try to resolve the complaint before it gets filed with OCR, he explains.

That doesn’t mean that when you field a complaint, you can insist on discussing a resolution before providing the OCR contact information. But you can offer to take steps to resolve the problem at the same time you make the contact information available.

That offer may convince the individual to let your facility handle the matter. And even if the individual still files a complaint with OCR, you have some warning and more time to prepare your response, he adds.

Dear newsletter subscriber,

Now, in addition to getting your monthly print newsletter, you’ll also get access to the online version and all its archives for FREE. Simply call customer service at 800/575-6787 or email at customerservice@hcpro.com and tell them you want electronic access. Each month, you’ll be able to read the latest information with a click of a few buttons.