HIPAA and Security

New Risks, Rules and Solutions

Security for confidential patient data is a growing problem, fueled by the rapid computerization of medical records and the Internet. In Michigan, for example, a student recently found thousands of patient records on the Web. Names, addresses, phone numbers, treatment details – available to anyone, no 'hacking' required.

This is one of many incidents where confidential patient data has been lost, sold, stolen and shared without authorization. Worried patients have petitioned Congress, and sued in court. DHHS Secretary Donna E. Shalala voiced a growing concern: "Will our health records be used to heal us or reveal us?"

In this white paper, we'll provide a concise review of the risks you face today, current laws and new HIPAA regulations – with solutions you can implement now. A directory of Web-based references is included at the end, for more information. *(Click on any URL in this document, to jump to the matching Web page.)*

A Unique Tradition of Privacy

Our medical records carry an unusual dimension and expectation of privacy. 2,000 years ago, the Hippocratic Oath required physicians to protect what they learned about their patients. Today we expect healthcare providers to follow the same pledge. As Janna Malamud Smith noted in Private Matter: The Defense of the Personal Life:

> " … few experiences are as fundamental to liberty and autonomy as maintaining control over when, how, to whom and where you disclose personal material."

Warning Signs

In a poll shortly before the November 2000 election, which issue was most important in the mind of the average voter -- crime, taxes, gun control, the economy, privacy or global warming? The surprising answer: privacy. We're bombarded by questions from employers, hospitals, insurance companies, credit card vendors … and the public knows: *all of that data goes somewhere*.

New HIPAA security regulations are simply a response to this rising concern. Year after year, surveys show that the public is *very* worried about the loss of confidential information, driven by computerization.

The Burden on Providers, Payors and Employers

This creates an unusual burden on the companies and people who manage healthcare information. If sensitive medical data is compromised, it's often *impossible* to fix the damage done to the privacy of the patient. Unlike financial fraud or credit card scams, no amount of money can balance the account and repair the loss.

Table of Contents:

The unique responsibility we carry with patient data is similar to secret military information. *One* confidential patient record released *one* time to the wrong party can cause significant and irreversible damage. Unlike a standard business system, more care must be taken at every step – from software development to operations.

It's the Right Thing to Do

Security often has a cold and negative feel -- the world of hackers and virus attacks. In health care, that's the disease and security is our cure. HIPAA sets a new standard of practice that's *good* news for patients – and good service for providers, payors and employers. Look for the positive benefits beyond the concerns:

- **It's Right for Your Patients:** Privacy for medical records is a basic human right. With loss of privacy at the top of the polls nationwide, it's clear that patients are worried – with good reason. Healthcare information systems are often not as secure as they should be. Improved security will give patients the protection they deserve.

- **It's Right for Physicians and Employees:** Everyone who creates and uses confidential patient information has an obligation to protect privacy -- that also carries some risk. Stronger security systems protect physicians, nurses, clerks and IT staff from liability and worry. Let your team know that better security is their ally and friend.

- **It's Right for Providers, Payors and Employers:** Every organization that works with confidential patient data has an obligation to protect privacy and potential liability. Improved security is your best defense against $millions in legal claims, and damage to your reputation that could never be repaired.

- **It's Right for You:** When you work to protect confidential patient data, you're fighting for the rights of every patient in your community. You're a key link in the "chain of trust". Everything you do to improve security will benefit and protect thousands of people – and help turn their concerns into confidence. This is a genuinely good cause.

Take the Lead: Get in front of the privacy issue -- with proactive answers that benefit the community and inspire confidence in your organization. Turn privacy concerns into a positive step forward.

Current Laws and Standards For Healthcare Data Privacy

A patchwork of existing laws protect patient data. Key regulations vary from state to state, and some types of patient data are specifically protected while others are not. New HIPAA privacy rules provide the national standard for confidentiality that is currently missing.

The interest in HIPAA, however, sometimes obscures the fact that we must comply *today* with all of the existing laws, regulations, accreditation requirements and professional standards, including:

> **JCAHO Information Management standards:** Scoring caps were removed from the Joint Commission's "Information Management" standards in 1998, and all organizations are expected to comply. Section IM.2 focuses on security and confidentiality of patient data. As the AHIMA noted in February of 2000, *"In the last year, there has been a particular focus on confidentiality"* in JCAHO's review process. The AHIMA provides a useful checklist of key issues:
>
> *Go to:* `www.ahima.org/journal/pb/00.01.html`

HCFA's updated Internet Security Policy: A complete explanation of current HCFA rules for transmission of patient data over the Internet, under the Privacy Act of 1974. If you want to transfer patient data via the Internet, this document outlines the types of encryption and authentication currently required by HCFA. **A must for every healthcare manager.**

Go to: www.hcfa.gov/security/isecplcy.htm

Note: The Privacy Act of 1974 applies to federal computer systems, not private systems. Patient data in your private computer system may be covered by HCFA policy, however:

" HCFA views this responsibility as a covenant with its beneficiaries, personnel, and health care providers. This responsibility is also assumed by HCFA's contractors, State agencies acting as HCFA agents, other government organizations, as well as any entity that has been authorized access to HCFA information resources as a party to a Data Release Agreement with HCFA."

State by State privacy laws: In 1999, the Health Privacy Project published a detailed and valuable review of healthcare privacy laws, on a state by state basis. Be sure to check this resource for specific regulations that apply in your location:

Go to: www.healthprivacy.org/resources/statereports/contents.html

Persons with disabilities: The Americans With Disabilities Act requires employers to maintain separate files for health questionnaires and medical examinations of applicants and employees. See section 12112(d)(3)(B).

Go to: www.eeoc.gov/laws/ada.html

Medicare patients: Medicare Conditions of Participation require providers to ensure the confidentiality of patient records. See 42 CFR 482.24(b)(3) and 42 CFR 486.306(o).

Go to: www.access.gpo.gov/nara/cfr/cfr-retrieve.html#page1

HIV related patient data: A new update published by the CDC in December of 1999 provides detailed instructions and procedures for the protection of HIV records.

Go to: http://www.cdc.gov/hiv/frn/hivctr.pdf

Organ donation: In February of 2000, HCFA restated rules for security related to organ donation and data collection. This useful document clarifies common misconceptions.

Go to: www.hcfa.gov/quality/4a1.htm

Immunization records: The National Vaccine Advisory Committee (NVAC) of the DHHS published updated rules in February of 2000, with detailed instructions for data security.

Go to: www.cdc.gov/nip/registry/download/cirman2.pdf

Mental health: The "Mental Health Bill of Rights" defines strict confidentiality standards for mental health and substance abuse treatment. Supported by the American Psychiatric Association, American Psychological Association and the American Nurses Association.

Go to: http://helping.apa.org/spreadtheword/rights.html

Drug and alcohol treatment records: Federal law provides privacy protection for people who receive drug and alcohol treatment at federally-funded clinics, including strict confidentiality rules for patient identity, diagnosis, prognosis and treatment. See: 42 CFR 290(dd-2).

Go to: www.access.gpo.gov/nara/cfr/cfr-retrieve.html#page1

Final HIPAA privacy standard: The 'final rule' for HIPAA privacy standards was published in the Federal Register on 28 December, 2000. This Department of Health and Human Services site offers online access to the complete rule, an easy-to-use fact sheet, and answers to common questions.

Go to: http://aspe.os.dhhs.gov/admnsimp/

The HHS fact sheet, outlining the final privacy rule:

Go to: `http://aspe.os.dhhs.gov/admnsimp/pvcfact1.htm`

Download the final rule in PDF format -- or view an HTML copy online:

Go to: `http://aspe.os.dhhs.gov/admnsimp/final/index.htm`

Standards vs. laws -- in a court of law

It's important to note that even if a professional standard does not a carry the "weight of law", it will still make quite an impact in the court room. The "Mental Health Bill of Rights", for example, isn't part of the Code of Federal Regulations – but imagine an attorney waving it in front of a jury. *"This is a well known and respected standard, available to anyone on the Internet! It's backed by every major professional association, but Mr. Smith ignored it, causing grievous harm to my client!"* These standards are often as important as laws to protect your patients, and can result in financial liability if they're overlooked.

Common Security Problems in Healthcare Information Systems

HIPAA has focused attention on an embarrassing problem: many existing healthcare information systems can't begin to meet basic security requirements. Protection is weak at best, and vulnerable to attack. When you audit your facility, look for seven common problems:

(1) **Always-on terminals and PC's:** You probably have dozens or hundreds of terminals and/or PC's scattered across your facility. Do *all* of them automatically go into a password-protected 'safe' mode if they're left unattended? If not, this is a classic open-door for security failure.

(2) **Weak passwords:** Many organizations do not strictly manage passwords. Common words like "password", "manager", the user's first name with one trailing digit, etc. are allowed – and they change rarely, if at all. Few organizations require security tokens or biometric ID.

(3) **No single sign-on with central management:** Many organizations have a jumble of different information systems, with *different* password databases. Most haven't implemented a "single sign-on" solution, and can't effectively manage passwords.

(4) **Weak security groups and limits:** Many systems allow any authorized user to launch any application, search for any record, and print a copy. "User groups" are often non-existent, or difficult to maintain. When these functions are available, many organizations don't bother to implement them.

(5) **Open databases:** The annual FBI study of IT crime shows that most break-ins are committed by people *within* the organization – a disgruntled employee, a curious student working part time, etc. The key weakness is often a standard "open" database, accessible via SQL and ODBC. (You probably *required* this in your last RFP.) Database security is often poor or non-existent, with no encryption, easily accessed with off-the-shelf reporting tools.

(6) **Weak PC management:** The Achilles heel of most healthcare networks is the same tool that improves worker productivity – the PC. Without stringent management, users can download applications from the Web, bring disks in from home, reset their security settings, etc. This is the most common path for viruses, Trojan Horse applets, and other security breakdowns.

(7) **Poor modem and Internet security:** How many PC's in your organization have their own modems, linked to a phone line? Is every dial-in router and WAN connection protected by a firewall? Without central management of all 'points of access', security is impossible to maintain.

New Security Threats From the Internet

The Web is rapidly becoming the ideal pipeline for healthcare data, allowing us to deliver patient records easily wherever they're needed, automate the payment process, and reduce costs. Patients and caregivers will have quick access to a host of useful resources, to improve the quality of care.

Every silver lining hides a cloud, and all of the benefits of the Web come with a significant cost. As your organization becomes linked to the Internet, doors open to a challenging world of security threats – from every corner of the globe. A hacker in Bulgaria may decide tomorrow that your system is an interesting target. When you connect to the Web, it's one big Party Line.

- **Email Vulnerability**
  Let's start with the most widely used tool on the Web -- email. Most organizations have an internal email server, and every employee has access to email applications and services. Many of your employees, allied physicians and patients also have *private* email accounts that can send and receive messages across your network, to your internal servers.

  Email systems create an open highway for privacy violations. Note eight key issues:

  (1) **No Security:** Most users and managers are not aware that email messages can be easily copied, read and modified as they move from server to server across the Internet. Many physicians, for example, send notes about their patients via email – with zero security. This violates HCFA regulations, and creates a significant risk of liability.

  (2) **Ownership:** Many employees do not know that the employer *owns* all of the email messages sent and stored on the employer's network, and has the right to read and monitor every email message. Without effective policies and notification, this can create significant conflicts in the workplace, disputes between employees, and legal costs.

  (3) **Discovery in a lawsuit:** Email has become a golden target for attorneys, as highlighted by the Microsoft / DOJ trial and recent troubles in the White House. Every email message stored on your server (and backup tapes) can be used against you.

  (4) **Offensive content:** Employers can be sued if employees send offensive messages via email, including sexual or racist content -- even if this clearly violates the company's email policy. For example, four female employees of Microsoft sued for alleged sexual harassment, which included pornographic email messages. Microsoft denied the charges, but settled for $2.2 million plus costs. In a similar case, a sexual harassment claim was filed against a subsidiary of Chevron Corporation when a list of "why beer is better than women" jokes circulated on the company's e-mail system. The claim was also settled for $2.2 million. (Have you seen similar 'joke' lists on your company's email system?)

  (5) **Spam:** Unsolicited commercial messages consume bandwidth and storage on your systems, and sap employee productivity. Spam is often linked to financial scams that can rob unsuspecting users, and pornographic sites that can lead to claims against your company. Often treated as an annoyance, spam is actually a serious problem.

  (6) **Viruses and security bombs:** Email messages can carry attached documents, HTML pages and applications that contain viruses and programs designed to blow holes in your security system. Email messages are easily broadcast and replicated, so infections can spread quickly. Email can also be stored on local PC's, making it very difficult to track down and completely eliminate a problem.

  (7) **Weaknesses in email servers:** Because email is the most widely used Web function, email servers are an obvious target for hackers. Significant holes have been found in every leading email system; your server may have 'back doors' that you're not aware of.

(8) **Threats from every corner:** Email messages can be sent by anyone, from anywhere. Even if you filter incoming messages to your email server, the address of the sender can be 'spoofed' with off-the-shelf utilities, to fool your system and your users. People with portable PC's may access email at home, with no protection, and carry a Trojan Horse into your network. This makes email an unusual threat, that's hard to pin down.

If you're not concerned yet, read "Email Woes" in the March, 2000 issue of InfoSecurity Magazine: `www.scmagazine.com/scmagazine/2000_03/cover/cover.html`

- **New Risks from Internet Access**

Most healthcare organizations provide access to the Internet via LAN or WAN. Like email, this is an important resource – with a host of security risks. The problems are similar:

(1) **Browser security:** Web technology is new and changing rapidly. A stream of security problems continue to pop up – and many users have not installed the 'patches' needed to plug these holes. Users can even turn security off when they run into problems with some Web sites. For an eye-opening review of issues, click on this Microsoft site, and read through the list of bugs: `www.microsoft.com/windows/ie/security/default.asp`

Browser flaws also affects your email systems. Many people don't know that HTML display functions used in OutLook, Eudora and other email systems are actually driven by Internet Explorer. When you open an HTML message sent via email, Outlook and Eudora *launch Explorer* -- and any weaknesses in Explorer are 'imported' into the email system.

This obviously creates a serious security problem for IT managers. Without strong and automated management of the browser on every PC in your system, you may have hundreds or thousands of holes in your security plan.

(2) **Personal Web surfing on the job:** The Web offers a world of distraction – from stock quotes to pornography. Your employees can spend hours on Web sites that have nothing to do with business. Is this a significant problem? From recent studies of Web use on the job:

- 50 percent of employees browse the Web for personal reasons
- One in eight men and one in nine women regularly visit sex-oriented sites
- 33 percent *frequently* download unauthorized software from the Web
- Average time spent per month on Web surfing: 20.3 hours

Clearly, personal Web usage is much more significant than most managers expect – consuming valuable time, and exposing employers to security risks and legal liability.

(3) **Malicious content:** Web sites can intentionally 'attack' a visitor, and copy confidential files from a PC or your network – with HTML tags, Javascript functions and ActiveX objects that compromise security.

(4) **Offensive content:** Like email, employers can be sued if employees openly cruise pornography sites or view other offensive material. The entire content of the Web, good and bad, becomes a legal concern for your organization.

(5) **Deliberate attacks on your network:** One of the beauties of the Web is the universal 'highway' it creates for information. This also creates a universal roadmap for attacks. Automated "sniffers" constantly cruise the Web, looking for vulnerabilities, holes and trap-doors that have been found in every leading system. A brute force "Denial of Service" assault can shut down your system without penetrating your firewall, driven by thousands of "innocent" computers on the Web.

An attack can be launched by a disgruntled employee, a hacker, a competitor, a bunch of bored teenagers in California, or a political group trying to make a statement.

If you think your Web site is secure, take a look at this recent attack on the popular New York Times site:

Before the attack

After the attack

Consider the resources of the New York Times. Does your IS team have *more* experience than theirs? This attack highlights how complex and difficult it can be to provide effective protection against intrusion.

(6) **New Threat - International Attacks:** As if there wasn't enough to worry about, the FBI's National Infrastructure Protection Center recently issued a warning about cyber attacks on U.S. Web sites, prompted by the on-going conflict in the Middle East:

> " The continued tension and increase in the number of cyber attacks shows no signs of abating… The NIPC recommends that recipients remain vigilant to the possibility that other U.S. sites may come under attack. It is anticipated that as the conflict in the Middle East continues, the level and severity of cyber attacks being experienced may escalate and expand."

This highlights the *international* nature of Web threats. An organized attack can be launched against your site from the other side of the globe.

For more info go to: `www.nipc.gov/warnings/advisories/2000/00-058.htm`

Myth #1: Who and Where is Your Top Threat?

New computer viruses make the evening news, with photos of hackers when they're caught. That's what most people think of, when they picture the people behind a security problem - smart young geeks with poor social skills, using the Web to break in and trash files.

Most people picture a hacker who looks something like this…

This is also a myth that leads people astray. The annual FBI study of computer crime points to an unexpected villain -- your own employees. Year after year, more break-ins are caused by employees than external hackers.

That's right, your #1 risk is *inside* your firewall, armed with an real ID badge and a password. This obviously compounds the problem. It's not enough to build walls to keep hackers out; your key risk comes from within.

… but the real threat is the ordinary guy you talked to in the hall today

Real world example: On December 1st, William Cox was sentenced to 6 months is jail for selling Tammy Wynette's medical record to the National Enquirer and Star. No teenage hacker, Mr. Cox is a well-educated, 35 year old researcher who worked for UPMC Presbyterian hospital. He obtained a copy of Wynette's record using a physician's password. (Sound familiar?) This is a classic example of the #1 risk in every organization.

Steps You Can Take Today to Improve Security

In this section, we'll walk through a series solutions you can implement today, to reduce risk:

- **Start with a review of policies and procedures**

  To improve compliance with existing law, and prepare for HIPAA, start with a review of your existing security environment and process – which will probably lead to some restructuring:

  (1) **Audit your organization:** This is the first step every organization should take -- call in a third party to perform an independent audit of your infrastructure, and find the holes. . An *independent* review is essential; your IT staff is too close to the systems they've implemented, and has a natural bias. If your audit is successful, you should find more problems that you expect. The results will become a powerful tool for change.

  We recommend TruSecure Corp., the publisher of Information Security magazine, and the leading authority on computer security assessment for a wide variety of industries. Like Underwriters Laboratories, TruSecure focuses on auditing and testing services. Unlike standard consulting groups, they don't sell services to help you fix the problems they find. (Which can create a revenue driven conflict of interest.) **For more info contact:** David Payne, TruSecure Corp., 703.453.0524 and visit their Web site at: www.trusecure.com

  (2) **Make sure your senior management backs security improvement:** The senior management of your organization must be convinced that privacy and security are significant and growing problems – strategic to survival, and worth their investment of time and money.

  (3) **Make security a requirement with every employee:** Many security problems are caused by lack of authority. If your IT staff is in charge of password management, for example, they may naturally be reluctant to go toe-to-toe with powerful physicians and department heads. Make sure compliance is a requirement from the top down.

  (4) **Appoint an Enterprise Privacy Manager:** Many organizations have a technical manager of security-related software, hardware and network access; if you don't, you should. It's also important to appoint a senior person to manage *overall* privacy policy, with the *authority* required to insure compliance throughout your organization.

  Your Privacy Manager should be backed by technical, administrative and legal resources, and should have primary responsibility for all privacy-related issues. For a useful job description, see the article recently published by the AHIMA:

  Go to: www.ahima.org/inconf/private.matters.0200.html

  (5) **Review and refresh your security policies and procedures:** You probably have a "security policy" of some kind – probably a section in your employee handbook, and a binder in your IS dept. Compare it to all of the laws and standards on page two, and make updates as required. Publish your updated policy on the new "Privacy and Security" section of your Intranet, with hyperlinks to current laws, and frequent updates to handle new threats.

  CPRI has put together an excellent no-cost toolkit to help you update your security policies and procedures, including basic training materials:

  Go to: http://www.3com.com/healthcare/securitynet/hipaa/toc.html

  The Health Privacy Project at Georgetown University also offers a review of healthcare privacy issues, with suggestions for improved privacy policies – that you can download at no charge:

  Go to: www.healthprivacy.org/usr_doc/33807.pdf

(6) **Spread the word:** The first step toward security is *awareness* and *buy-in*. Security solutions are often less convenient, and often seem unnecessary to many users. Your team needs to believe that the threats are real, and worth their attention.

Setup a 'privacy and security' page on your Intranet. Include a link to www.infominers.com, to give them online access to all of the resources in this document. Start a 'privacy bulletin', with weekly updates via email.

(7) **Prepare to invest in expertise and technology:** Some risks can be eliminated with policy and procedure changes. Others will require sophisticated technology and expertise, including encryption, firewalls and management systems. Even if you have a large organization with lots of resources, you'll need advice and tools from people who make security a daily business.

You'll also need to boost your budget for security hardware and software, including technical training for your team. To see where you stand compared to the current "best practices" across the IT industry, see this March, 2000 write-up in Network Computing magazine:

Go to: www.nwc.com/1105/1105f2.html

- **Improve protection for your existing information systems and databases:**

The second step toward risk reduction and HIPAA compliance will improve protection for your patient data, and reduce potential legal liabilities – immediately:

(1) **Install password protected 'secure desktop' software on every PC:** 'Secure desktop' software will automatically time-out to a password protected screen-saver, if left unattended. Centrally managed solutions are available from a number of vendors, including the Zero Administration kit from Microsoft™ for Windows 98™, NT and 2000.

(2) **Mandate more effective password control:** Your security audit should uncover and document the way passwords are being managed. The focus is typically on user convenience, not security. Educate your users on the fundamental importance of passwords, and implement new procedures to (1) automatically create more complex passwords that cannot be easily guessed, and (2) refresh all passwords frequently.

(3) **Talk to your system vendor about improved security:** Make sure you've fully implemented the security functions included in your existing systems. With HIPAA on the horizon, your vendor probably has improved security functions in the works, including central password and 'rights' management.

(4) **Explore purchase of a single sign-on system:** If your users need to access a number of different systems with different passwords, take a serious look at the purchase of a single sign-on system. These solutions aren't cheap, and require installation effort – but without one, it's extremely difficult and time-consuming to maintain a secure environment.

(1) **Improve protection for all 'open' databases:** Your audit should provide a detailed list of all databases that contain patient information, with a particular focus on systems that use a standard 'open' database that supports SQL and/or ODBC, e.g. Microsoft Access™, SQL Server™, Oracle™, Paradox™, Informix™, Btrieve™, etc. With a thorough audit, larger organizations often find that dozens of databases have popped up here and there, to support departmental applications, local reporting, etc. – and they're rarely secure.

Try to move these databases, where possible, to 'hardened' and secure servers that are centrally managed, and physically protected. If a database must remain in a departmental office, it should be moved to a hardened server that is centrally managed, with some form of physical security.

As you dig deeper into this problem, you may find that this a good time to 'retire' departmental reporting systems, and create a shared data warehouse. Your users still run their standard reporting tools, but the data will be stored in a more efficient and protected environment.

(6) **Install a central PC management system:** If your organization has more than a dozen PC's, this is the most critical step you can take toward effective security. No matter what else you do, your security plan will fail if PC's on your network are unmanaged and unaudited.

For many organizations, this is a big step that requires a change in culture, in addition to software and training. Users treasure the independence they feel with "their" PC, and are loath to surrender control. Make sure your IT team is thoroughly trained, and educate users before you start.

If you don't provide constant, detailed management of your PC's today, be prepared to add staff. There's no better prescription for user revolt, than a central management system that's understaffed and poorly managed! Make sure users have a strong voice in the process.

Central management systems for PC hardware, operating systems and software are available from a number of leading vendors, including Microsoft and Computer Associates.

(7) **Lock down external access routes:** Your audit should document every modem and phone line that users can access, and you should completely ban any access that doesn't go through your secure servers, filters and firewalls. This should be backed by strict enforcement.

- **Secure your email services:**

(1) **Clarify your email policy:** Many employers don't have an effective e-mail policy, and recent court cases underscore the risk of inaction. Review and update your email policy, notify your employees, and post a copy on your Intranet site. For an example of a good policy with legal background on key issues, see: www.morganlewis.com/art61499.htm

(2) **Train and remind your employees and users:** Publish a weekly bulletin to every email user, noting new email virus threats, attachments to avoid, and email policy issues. Add a similar 'bulletin' section to your Intranet site, in a prominent location. This will help to keep security concerns fresh in your user community. Automated systems will help you manage this process – see the list on the next page.

(1) ***Require* email encryption, particularly for physicians working with patient data:** It's easy to make email secure with off-the-shelf encryption products. This is *essential* for physicians who use email to contact patients, consult with colleagues, etc. Solutions include add-ons for common email products, e.g. Outlook™ and Eudora™, and complete email systems with secure clients and servers – see the list on the next page.

Notify your physicians, spell out the *current* HCFA requirements, and remind them with regular email bulletins. If you have a Web site or an Intranet page specifically for physicians, add a prominent 'security for patient data' section, with the latest info. Include the ability to download an encryption add-on for their email package, at no charge. Offer special training sessions for physicians, to explain the threats and solutions.

(4) **Install an automated email encryption / monitoring system:** This is one of the most important steps you can take to secure your entire network – **every healthcare organization should install a system** that will automatically encrypt email, scan for attached viruses, filter spam and objectionable content, etc. Some will also help you define and update your email policy, train users, distribute bulletins, etc.

Note four highly-rated email management solutions:

MIMEsweeper™	*Go to:* www.us.mimesweeper.com/products/websweeper/
CommandView™	*Go to:* www.elronsoftware.com/productfamily/msginspector.shtml
MailMarshall™	*Go to:* www.cleane-mail.com/
MailGuardian™	*Go to:* www.vguard.com/index.asp

Also take a look at a recent review of email management products:

Go to: www.check-mark.com/securecomputing/2000_03/testc/prod1.html

- **Secure your access to the Web:**

(1) **Clarify your policy for Web use:** Like email, many employers don't have an updated policy for Web usage. Review and update your policy, notify your employees, and post a copy on your Intranet site. The example provided on the previous page for email also includes terms for Web usage: www.morganlewis.com/art61499.htm

(2) **Train and remind your employees and users:** Most users are aware of viruses in email, but many do not know that malicious Web sites can launch an attack directly through your Web browser – without opening an 'attachment' or clicking on anything. Explain the risks, and the importance of updating the version of the Web browser they use.

(3) ***Require* use of a standard 'managed' Web browser, particularly for physicians working with patient data:** This is one of the most important steps you can take to improve security in your organization – require the use of a standard Web browser, and provide automated updates.

There are some challenges to effective management. The full update to a new browser version may require the user to load a CD – the files are typically 30+ megabytes, and difficult to download. The new browser may also require end-user training. Patches to security holes must also be applied regularly. Bottom line: although the Web is the most convenient and cost effective way to provide access to patient data, management of secure Web browsing isn't convenient, easy or cheap.

Note these sites for the latest information on Microsoft™ and Netscape™ browsers:

Internet Explorer™ *Go to:* www.microsoft.com/windows/ie/security/default.asp

Netscape™ *Go to:* www.netscape.com/download/index.html

(4) **Install an automated monitoring and content management system for Web usage:** This is one of the most important steps you can take to secure your entire network – **every healthcare organization should install a system** that will automatically track, scan and filter Web traffic for non-business usage and malicious or objectionable content, etc. Some will also help you define and update your policy for Web usage, train users, distribute bulletins, etc.

Note two highly-rated Web content management solutions:

WebSweeper *Go to:* www.us.mimesweeper.com/products/websweeper/index.htm

SurfControl *Go to:* www.surfcontrol.com/products/index.html

Also take a look at a recent review of Web content issues and management products in the March 21,2000 issue of Network Computing:

Go to: www.networkcomputing.com/1103/1103f2.html

(5) **Install high-quality firewall and intrusion detection system:** You probably have a firewall system in place, to protect the link between your network and the Web. In your security audit, make sure this system is up to date. Firewall technology is constantly changing to meet new threats, and if your firewall is more than a year old, you should take a close look at a major upgrade or replacement. Also check to see if your IT staff is fully trained on firewall management.

If you don't have an "intrustion detection" system, add one immediately. These systems monitor the activity on your network automatically – and watch for unusual events that could signal a break-in. Although not perfect, this final line of defense should be a critical part of your Web strategy. For a review of issues and products, click on this article from Network Computing magazines: *Go to:* www.networkcomputing.com/1010/1010r1.html

(6) **Install a Virtual Private Network for links to sensitive patient data:** For links to patient information, you should provide another layer of protection. Virtual Private Network systems (VPN's) create a "private line" over the public Internet. Data is encrypted during transmission, and special software is required on both ends to make a connection. This separates your links to patient information from ordinary Web traffic. VPN systems also support digital certificates and more effective user ID – both key requirements in pending HIPAA regulations.

(7) **Evaluate biometric ID systems:** One of the basic challenges with security is the identification of the user. If the PC is inside your facility, you have greater control. If someone is dialing in via the Internet, how can you verify the identity of the person on the other end of the line? Ordinary passwords? This is hardly effective, and difficult to manage. Biometric ID systems take the next step, and ID the user based on a fingerprint, iris pattern, etc. This provides much tighter control over authorized access – and eliminates the hassle and cost of password management. User ID is a key requirement with HIPAA, and biometric systems should be part of your plan.

(8) **Upgrade security training for your IT staff:** This basic step is often overlooked. Web security is very complex and changes rapidly. Your plan should include a significant amount of security training for an IT Security Team, with refreshment courses throughout the year. I recommend at least one class per quarter for each person. These courses are often relatively costly, by the way, so make sure you leave room in your budget.

(9) **Consider out-sourcing Web security functions:** If your organization doesn't have the resources to handle the daunting challenges of Web security, don't despair – and don't try to "make do". One of the beauties of the Web is the ability to out-source. Your secure Web server could be installed at your site, or a 1,000 miles away. Users can't tell, and they'll often receive faster Web access than you could provide from your own facility.

Out-sourcing eliminates the need to install and maintain complex security hardware and software, hire additional staff (a real challenge in this economy) and support security technology. From a management point of view, it's often easier for a third-party to introduce and control user access – an irate physician who doesn't want to change his/her Web browser, for example, can't pressure your IT staff. It's out of their hands.

Prepare for HIPAA Compliance

The Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), promises to fuel some of the most far-ranging and costly changes ever seen in healthcare IT. Over the next few years, the total cost of HIPAA compliance will exceed the cost of Y2K updates – with significant changes to existing software, and extensive consulting services.

HIPAA focuses on three areas:

1. **Standardized coding** for electronic data interchange (EDI) transactions – to facilitate the easy exchange of patient data between systems, with greater efficiency
2. **Strict new security standards**, designed to protect confidential patient information
3. **New 'unique identifiers'** for providers, payors and employers

Improved security for patient data is one of the key elements of proposed HIPAA regulations, creating a consistent and much-needed national standard for confidentiality. Here's a quick overview of HIPAA security requirements:

Security Function	Notes:
Access control	• Emergency access required • Must support access based on the user, role or context. • Encryption is technically optional, but required in a practical sense
Audit control	Audit control mechanisms must record and examine system activity, to identify suspicious data access activities, assess your security program, and respond to potential weaknesses

(continued…)

Security Function	Notes:
Authorization control	Must include a mechanism for obtaining consent for the use and disclosure of health information. Can include either role or user-based access.
Data authentication	Must be able to prove that data has not been altered or destroyed in an unauthorized manner, e.g. via. check sum, double keying, message authentication code or digital signature.
Entity authentication	• Must support automatic log off. • Must support unique user identification. • Must implement one of the following: biometric ID, passwords, PINs, telephone call-back or security tokens.
Patient access to records	Patients must be able to see and get copies of their records, and request amendments.
Disclosure logs	A history of most disclosures must be made accessible to patients. (This is a very challenging requirement -- all access and disclosure must be logged, and must be easy to access.
Data communications	• Must support integrity controls • Must support message authentication • Must implement one of the following: encryption or access controls
Network communications	Must support alarms, audit trails, entity authentication and event reporting.
Electronic signature	• Must provide message integrity • Must support non-repudiation • Must support user authentication
Data release	• Must support de-identification of patient data • Must support release of the minimum amount of personal data needed for a particular authorized user • Includes very specific rules governing release in a variety of situations, e.g. business partners, public health, law enforcement, research, etc.
Privacy Manager	Organizations must designate one 'privacy official' to manage regulatory issues, with a formal process to handle complaints, etc.
Civil Penalties	• Health plans, providers and clearinghouses that violate these standards would be subject to civil liability. Civil money penalties are $100 per incident, up to $25,000 per person, per year, per standard.
Criminal Penalties	• Wrongful disclosure: $50,000, imprisonment of not more than one year, or both. • Offense under false pretenses: $100,000, imprisonment of not more than 5 years, or both. • Offense with intent to sell information: $250,000, imprisonment of not more than 10 years, or both.

Important Changes Added to the Final Rule

After extensive review and public comment, a number of important changes were added to the final version of the HIPAA security rule, including:

- ***All forms* of personal medical data** are now covered, including electronic and paper records -- even oral communications. The preliminary rule covered only electronic data and medical records.
- **Covered entities now include**: health plans, health care clearinghouses, and health care providers who conduct certain financial and administrative transactions (e.g., electronic billing and funds transfers) electronically. "Providers" are broadly defined, and include a wide variety of entities, e.g. pharmacies, labs and ambulance services.
- **Patient consent is required** before information can be released, even for routine disclosures. Detailed procedures must be followed. (The preliminary rule permitted "routine" disclosures.)
- **Medical data cannot be used for employment purposes**, without specific authorization. Companies that sponsor health plans, for example, cannot access the personal health information held by the plan for employment-related purposes, without authorization from the patient

Steps You Can Take Today

Looking through all of these requirements, and the potential penalties, it's clear that (1) this is a serious and comprehensive effort to improve security across the board, and (2) compliance won't be easy to implement. Consider the following steps, which you can begin to implement today:

(1) **Implement basic security improvements:** All of the steps outlined previously will improve security and reduce your legal exposure today, and put you well on the road to HIPAA compliance.

(2) **Include HIPAA in your security audit and plan:** One of the first steps we outlined was a general security audit and upgrade plan. As you examine your existing systems and procedures, keep HIPAA compliance in mind. Note obvious problems and potential deficiencies.

(3) **Launch discussions with your existing vendors:** Legacy information systems will be one of the most difficult areas of compliance. Many of these systems were never designed with high level security in mind, and changes will be difficult. When patient data is transmitted it is not well protected, databases are not encrypted, password systems are weak and typically do not include audit trails, and no authentication/non-repudiation is provided for data access. Launch discussions with your vendors as soon as possible, to uncover their plans for compliance -- and the costs you should expect to pay. Many will probably require major system upgrades.

(4) **Plan to install a VPN, advanced firewall and intrusion detection:** Some of the more advanced steps at the end of our general security plan will be particularly useful for HIPAA compliance. A good Virtual Private Network (VPN) for example, will include all of the digital signature, encryption, non-repudiation and logging functions noted in the HIPAA proposals.

(5) **Consider hiring expertise:** For many consulting companies, HIPAA looks like "Y2K Round Two". They see a gold mine of billable hours under all of those regulations, particularly from organizations that delay and dawdle. This doesn't mean that you shouldn't consider hiring some help, however. Security technology is notoriously complex, and most healthcare organizations simply don't have the resources or training required.

(6) **Keep an eye on those HIPAA Web pages:** The final HIPAA rule was published on 28 December, 2000. Watch for a flood of analysis and commentary from across the industry -- with useful tips and information.

Summary

As we noted at the beginning, don't allow future compliance with HIPAA to overshadow the basic issues you face today: the patient data you're responsible for is often protected by law *now*, and you face a very real risk of legal and financial liability -- today. Many of the HIPAA requirements simply reflect good security practice, that everyone should implement with or without federal regulation.

Get started today.

HIPAAwire Quick access to Web resources and current security news:

For convenient access to HIPAA resources and the information, go to HIPAAwire, an information oriented portal covering security issues for the healthcare industry. All of the Web links included in this whitepaper are available at HIPAAwire, along with new information on security threats and solutions.

Go to: `www.ingenix.com/hipaawire`

Email if you have questions:

`Mark.Hays@ingenix.com`

A directory of resources for HIPAA security is attached:

A directory of resources for security and HIPAA is attached. More than the usual list of Web links, each of these sites and documents has been reviewed in detail for quality and content. You'll find a wealth of helpful information. (To avoid typing in the URL's, the Web links can be accessed quickly via HIPAAwire -- click on the links shown above.)

HIPAA security solutions from Ingenix:

Ingenix offers a family of security solutions that cover all of the issues related to HIPAA compliance, including security, standards for healthcare data and EDI transactions, etc. Please contact us for more information. Phone: 801.536.1000 and ask for Mark Hays or send email to `Mark.Hays@ingenix.com`.

About the author:

Mark Hays has more than 15 years of experience with security technology, including military / defense systems. He co-authored a number of patents for secure software, including key management for Public Key cryptography. Mark received a First Place award from Bill Gates for the Best Healthcare Application for Windows, a First Place at the Microsoft Healthcare Users Group, and a First Place in Healthcare/Biotechnology at Uniforum.

Mark serves as the CTO for Ingenix, where he directs development of security solutions, e-commerce systems and Web based applications.

Mark welcomes your comments and questions. Please email to: `Mark.Hays@ingenix.com`

Bill Gates and Mark Hays at Windows World

A Directory of Web Resources

Real-world Examples of Confidentiality Problems:

A Connecticut physician discovers that a pharmaceutical company is using his patient's prescription data to market a new drug.

Go to: www.newstimes.com/archive98/nov1098/rgh.htm

An Ohio psychologist ends up in court, trying to protect his patient's medical record from a self-insured employer.

Go to: www.apa.org/monitor/sep99/in3.html

Is your medical record secure? This recent article in USA Today lists a series of incidents where patient information was lost, shared with employers, and sold to pharmaceutical companies.

Go to: www.usatoday.com/life/health/online/lhonl032.htm

The Washington Post uncovers an agreement between pharmacy giant CVS and major pharmaceutical manufacturers, to use personal prescription data to market drug products.

Go to: http://washingtonpost.com/wp-dyn/articles/A99149-1998Feb15.html

CVS and Glaxo Wellcome face a class-action lawsuit, alleging that they used prescription data to market drugs to patients.

Go to: www.directmag.com/magazines/directnewsline/OldArchives/199803/1998032701.html

Thousands of medical records from the University of Michigan Medical Center are left on a public Web site -- for months.

Go to: www.nurseweek.com/news/99-2/22d.html

Email nightmares -- the cover article in the March, 2000 edition of InfoSecurity Magazine:

Go to: www.scmagazine.com/scmagazine/2000_03/cover/cover.html

Reports on Confidentiality from JCAHO, NCQA, AHIMA, CDC and AMA:

NCQA and JCAHO released this joint report on confidentiality and patient data in November of 1998, the result of a study funded by the W.K. Kellogg Foundation and DHHS. This is a thorough and detailed report on key issues, with recommendations.

Go to: www.ncqa.org/pages/communications/news/tablcont.htm

Download a copy of the entire report at: www.ncqa.org/pages/communications/news/confrel.htm

JCAHO published this annotated version of the joint NCQA/JCAHO report in December of 1999, which noted, "Security audits are common in other industries and government agencies and these methods can be adapted to the health care industry." A sign of things to come.

Go to: www.jcaho.org/pphi/7recmmnd.html

AHIMA's position paper on confidentiality, with a thorough but concise review of key issues, and good examples. Very useful.

Go to: www.ahima.org/infocenter/current/white.paper.html

AHIMA review of patient confidentiality bills currently before Congress, with evaluations and comparisons.

Go to: www2.ahima.org/pdf_files/senate106b.pdf

American Medical Association review of confidentiality, with recommendations.

Go to: http://jama.ama-assn.org/issues/v282n15/abs/jlm80037.html

AMA policy statements regarding HIPAA EDI standards for claims/encounter and CPT data, and "Fraud and Abuse" provisions.

Go to: www.ama-assn.org/med-sci/cpt/hipaa.htm

CDC report on confidentiality and the public use of health statistics, from the National Center for Health Statistics.

Go to: www.cdc.gov/nchs/otheract/phdsc/presenters/gostin.htm

The President's Advisory Commission on Consumer Protection and Quality in the Healthcare Industry published this "Consumer Bill of Rights" statement in 1998, which includes a review of confidentiality laws and proposed standards. A useful review of key issues.

Go to: http://health.upenn.edu/aging/diverse/president.shtml

American College of Physicians- American Society of Internal Medicine (ACP-ASIM) position statement on proposed HIPAA confidentiality rules. Outlines concerns about the potential burden of HIPAA on independent physicians and small practices.

Go to: www.acponline.org/hpp/privacylet.htm

HIPAA -- General:

Final HIPAA privacy standard: The 'final rule' for HIPAA privacy standards was published in the Federal Register on 28 December, 2000. This Department of Health and Human Services site offers online access to the complete rule, an easy-to-use fact sheet, and answers to common questions.

Go to: http://aspe.os.dhhs.gov/admnsimp/

Download the final rule in PDF format -- or view an HTML copy online:

Go to: http://aspe.os.dhhs.gov/admnsimp/final/index.htm

The main HCFA web site for HIPAA, with a good overview and detailed information for consumers, employers and health plans.

Go to: www.hcfa.gov/medicaid/HIPAA/default.asp

HIPAA -- Key Professional Organizations:

American Health Information Management Association (AHIMA)

Go to: www.ahima.org

Computer-based Patient Record Institute (CPRI)

Go to: www.cpri.org

Be sure to download the excellent (and free) CPRI toolkit "Managing Information Security in Healthcare". *Go to:* www.cpri-host.org/resource/toolkit/toolkit.html

(HIPAA - Key professional organizations -- continued…)

Health Insurance Association of America (HIAA) Web site, a trade association that represents the private health care industry, including healthcare providers, long-term care, disability, dental, and supplemental coverage.

Go to: www.hiaa.org/

American Medical Association (AMA) Web site, which focuses on physician-related issues, and new clinical research/treatment results.

Go to: www.ama-assn.org/

The Health Privacy Project (HPP) Web site, founded by the Institute for Healthcare Research and Policy at Georgetown University. This very helpful site includes a detailed analysis of key issues, and valuable resources -- including a unique national study of state healthcare privacy laws. **A key resource.**

Go to: www.healthprivacy.org

Be sure to download the HPP's thorough 1999 review of healthcare privacy issues, with specific suggestions for improved privacy policies.

Go to: www.healthprivacy.org/usr_doc/33807.pdf

HIPAA -- Security:

Download a free evalution handbook for HIPAA security, from the Electronic Healthcare Network Accreditation Commission, an independent non-profit accrediting group. EHNAC establishes criteria for clearinghouse and value-added network performance, and is in the process of establishing a "HIPAA Security Accrediatation" process.

Go to: www.ehnac.org/SecurityAccreditation/Default.html

A useful collection of security resources and information related to healthcare data, from the Massachusetts Health Data Consortium.

Go to: www.mahealthdata.org/

A thorough review of Unique Patient Identifier options and issues, from the AHIMA.

Go to: www.ahima.org/publications/2f/feature.1099.2.html

HIPAA -- EDI:

WEDI (Workgroup for Electronic Data Interchange) has organized many of the discussions related to new standards for EDI in healthcare, including the standards now enacted as part of HIPAA.

Go to: www.wedi.org

Information on standards for EDI (Electronic Data Interchange) from the ASC X12 group. This is a key part of HIPAA, which will standardize transactions between systems, e.g. for healthcare claims.

Go to: www.x12.org

Download free X12N implementation guides for HIPAA-compliant EDI. WPC is the official publisher for the ASC X12N, which develops and approves the EDI guides.

Go to: www.wpc-edi.com/HIPAA_40.asp

(HIPAA - EDI -- continued…)

A detailed and useful guide to EDI projects, from the Massachusetts Health Data Consortium. Includes a sample cost / benefit analysis, tips for vendor and system evaluation, and a valuable collection of worksheets to guide the implementation of an EDI project.

Go to: www.mahealthdata.org/mhdc/report2.nsf/edi?openview&count=40

An industry group that promotes the use of standard XML transactions for electronic commerce. Originally founded by Microsoft, this group is independent and supported by technology vendors like SAP, and users like Boeing and BP/Amoco. You can download useful guidelines and examples showing on how to use XML to exchange data between different systems.

Go to: www.biztalk.org

HIPAA -- Consumer Guides to Health Insurance Coverage:

View and download consumer guides describing your right to buy and keep health insurance under HIPAA, with details on the specifics in each state. Includes a Spanish version.

Go to: www.georgetown.edu/research/ihcrp/hipaa/

Web Security References:

Monitoring employee email in the Internet Age: an excellent review of legal issues related to email and the Internet, with useful examples and references to court cases. Legal orientation.

Go to: www.morganlewis.com/art61499.htm

Web usage by employees: a detailed report on current Web usage patterns, including personal Web browsing on the job.

Go to: http://cyberatlas.internet.com/big_picture/traffic_patterns/article/0,1323,5931_322381,00.html

1999 Privacy Law Sourcebook: a comprehensive and useful review of current privacy law, including new developments related to the Internet.

Go to: www.epic.org/pls/

Bills currently in Congress related to privacy: Nothing attracts the attention of Congress like millions of vocal online voters, and a host of bills are currently in play related to privacy on the Web, patient records, etc. It's important to keep an eye on these developments. This useful site lists all of the bills currently before the House of Representative and the Senate.

Go to: www.epic.org/privacy/bill_track.html

Court rules that cryptography is protected by the First Amendment: the U.S. Court of Appeals for the Sixth Circuit ruled on April 4, 2000 that cryptography software is protected by the First Amendment.

Go to: http://pacer.ca6.uscourts.gov/cgi-bin/getopn.pl?OPINION=00a0117p.06

Download a free "anti-spoofing" test tool from AIS, to make sure your network can't be exploited for a DoS attack.

Go to: www.icsa.net/html/communities/ddos/alliance/checker/index.shtml

Organizations and Web Sites Focused on Security:

Alliance for Internet Security, which focuses on prevention of Denial of Service (DoS) attacks on Web sites. Sponsored by ICSA.net, with members that include Information Security Magazine, Computer Associates, the Department of Veterans Affairs, and many Internet-related companies.

Go to: www.icsa.net/html/communities/ddos/alliance/index.shtml

Electronic Privacy Information Center (EPIC): an excellent source of information on evolving security issues, laws and court cases related to the Internet and computerized data.

Go to: www.epic.org/

SANS Security Institute: This non-profit organization was founded in 1989, and their Web site provides extensive information on security technology, issues and solutions. Technically oriented.

Go to: www.sans.org

Weekly e-mail bulletins from the SANS Institute: This valuable service will send you free weekly bulletins on the latest security issues, virus alerts, etc. **A must for anyone concerned with security solutions.**

Go to: www.sans.org/sansnews

Microsoft security Web site: The latest info on security problems, new patches for Microsoft products, and useful reviews of common security issues.

Go to: www.microsoft.com/technet/security/default.asp

E-mail security bulletins from Microsoft: Go to this site to signup for automatic security bulletins from Microsoft. **A must for anyone who manages Microsoft-based applications and servers.**

Go to: www.microsoft.com/technet/security/notify.asp

Netscape security Web site: The latest info on security problems, new patches for the Netscape Web browser, and useful reviews of common security issues.

Go to: http://home.netscape.com/security/index.html

ICSA Security Site: Publisher of Information Security magazine, ICSA.net is a recognized authority in security threats and solutions. Technically oriented.

Go to: www.cert.org/index.html

The ICSA.net Hype-or-Hot meter: Gives you the latest on real Web security threats, and fakes.

Go to: www.icsa.net/html/hypeorhot/index.shtml

CERT Security Site: CERT is part of the Survivable Systems Initiative at the Software Engineering Institute, a federally funded research and development center at Carnegie Mellon University. CERT tracks attacks on computer systems, and the site offers information on security issues. Technically oriented.

Go to: www.cert.org/index.html

W3C Security Resources Site: The World Wide Web Consortium, founded in October of 1994 by Web inventor Tim Berners-Lee, is the leading organization for Web standards. The W3C provides a Security page with lots of useful information.

Go to: www.w3.org/Security/

NIST Security Site: The National Institute of Standards and Technology operates a Computer Security Resource Clearinghouse (CSRC) with the latest information on security issues:

Go to: http://csrc.ncsl.nist.gov/

National Security Agency glossary of security terms: Puzzled by another acronym? This glossary defines and explains a wide variety of security terms. You can quickly lookup topics by name. (This is a large HTML file, which takes a couple of minutes to download – don't worry if your Web browser appears to "lock-up" while the page is being transferred.)

Go to: www.sans.org/newlook/resources/glossary.htm

Information Systems Audit and Control Association Site: With 21,000 members worldwide, ISACA administers the CISA® (Certified Information Systems Auditor™) designation, and develops global auditing standards for information systems.

Go to: www.isaca.org/

Uniform Electronic Transactions Act: a public forum on Federal law governing Internet transactions. Sponsored by the National Conference of Commissioners on Uniform State Laws, which developed the Uniform Commercial Code, in a joint project with the American Law Institute.

Go to: www.webcom.com/legaled/ETAForum/

Industry Magazines Focused on Security:

InfoSecurity magazine: A leading digital security publication, in three languages.

Go to: www.scmagazine.com/index2.html

Network Computing magazine: A leading publication, with good product reviews.

Go to: www.networkcomputing.com/

Recommended Security Product Reviews by Leading Magazines:

InfoSecurity magazine, Buyer's Bible for 2000:

Firewall software:	www.scmagazine.com/scmagazine/1999_12/buyers_bible/p_firewall.html
Internet security:	www.scmagazine.com/scmagazine/1999_12/buyers_bible/p_internet.html
Access control:	www.scmagazine.com/scmagazine/1999_12/buyers_bible/p_access.html
Anti-virus:	www.scmagazine.com/scmagazine/1999_12/buyers_bible/p_antivirus.html
Intrusion detection:	www.scmagazine.com/scmagazine/1999_12/buyers_bible/p_intrusion.html
Network security:	www.scmagazine.com/scmagazine/1999_12/buyers_bible/p_network.html

Network Computing magazine:

Firewalls:	www.networkcomputing.com/1023/1023buyers2.html
Desktop encryption:	www.networkcomputing.com/819/819r1.html
VPN solutions:	www.networkcomputing.com/1010/1010buyers2.html
Anti-virus gateways:	www.networkcomputing.com/1105/1105buyers2.html

Internet Week magazine:

Firewalls:	www.internetwk.com/reviews00/rev022100.htm
Content filtering:	www.internetwk.com/reviews00/rev041700-1.htm