

**NEWS**  
browser.

To print this page [click here](#), or select "Print" from the "File" menu of your

Dec. 2005

**Network Security: Protecting Patients and Patient Data**

*Many healthcare organizations are grappling with the consequences of HIPAA and with the reality of operating in today's turbulent security environment. HealthLeaders contributor Mitchell Ashley says healthcare organizations need to evaluate their network and implement a blend of security measures that provides the highest level of protection given the available resources.*

Healthcare organizations face serious challenges when implementing information technology. A network or data security incident can have catastrophic consequences. IT professionals are familiar with scenarios in which a security attack can set an organization back weeks or months and cost hundreds of thousands—even millions—of dollars to fix. However, the real nightmare scenarios are just beginning to be discussed: a cyber-terrorist gaining access to patient data and changing lab scores, physician diagnoses, and medication doses. In such scenarios, "catastrophe" takes on a whole new meaning.

Today, with so much confidential patient data stored and processed digitally and the risks of a security breach growing exponentially, protecting information is a paramount concern for healthcare organizations. One only need take a look at some of the high-profile healthcare security breaches to see why protecting information has become a business and technology priority. In August 2005, more than 300 radiotherapy patients were turned away from a hospital in Bebington, in the United Kingdom, after a computer virus infected the network. In June 2000, a hacker penetrated the University of Washington Medical Center's internal network and downloaded names, addresses, birth dates, social security numbers, heights and weights of more than 4,000 heart patients, along with each medical procedure they underwent.

Today, every healthcare organization must address the following potentially far-reaching questions:

- Are confidential patient records truly secure?
- How can networks be secured with limited IT budgets and resources?
- What are the consequences of noncompliance with HIPAA and other applicable privacy regulations? What steps should be taken to ensure compliance?

**The Health Insurance Portability and Accountability Act of 1996**

Designed to protect the confidentiality and integrity of electronic personal health information, HIPAA has redefined how healthcare providers handle private patient data. HIPAA is not a check-box that organizations can take off their "to do" list once complete. Although HIPAA regulations are already in effect, compliance can only be achieved over time. HIPAA requires ongoing processes and procedures that enforce the security of patients' personal health information. Most healthcare organizations were required to comply with HIPAA's security provisions by April 21, 2005. They are now focused on making progress by using updated procedures and solutions to establish controls for enforcing mandated security measures applying to patient, billing, and insurance information.

HIPAA security legislation requires policies, procedures, and documentation as well as technical and physical safeguards. In its revised form released in February 2003, HIPAA regulations focus on providing security management principles, as opposed to specific technology implementations. HIPAA references a number of National Institute of Standards and Technology security standards that healthcare organizations should follow. The legislation is results-focused, and cost is not a reasonable excuse for noncompliance.

**Complex IT Environments and Resource Constraints**

Information security at healthcare organizations typically includes management of complex networks comprised of powerful servers or mainframes, desktops, "thin" computers, and mobile devices. Controlling access to these networks is a daunting task, and the challenge becomes even more difficult when budgets are tight and resources are at a premium, as is common within the industry.

In addition, information security is often one of many responsibilities for a healthcare network administrator. Operating under these collective pressures, network administrators need strong top-down security policies, cost-effective, dependable solutions that enable efficient security management and airtight incident response procedures when events occur.

### **Implementing a Network Security Program**

Many healthcare organizations are grappling with the consequences of HIPAA and with the reality of operating in today's turbulent security environment. A healthcare organization's network security program needs to start at the executive and board level. A clear, concise network security policy needs to be drafted that accounts for the organization's size, goals, and infrastructure while complying with HIPAA. A sound policy with buy-in from the top brass is critical so that network administrators don't get push-back during policy and solution implementation.

Organizations should take a best practices approach to their network security policy that ensures they are following common processes for security implementation. The current best-practices standard recommends a layered security approach that provides in-depth defense against any potential security breaches.

To better explain the best practices approach to network security, we should first explain the hacker's "work factor," which is an important concept when implementing layered network security. Work factor is defined as the effort required for an intruder to compromise one or more security measures, which in turn allows the network to be successfully breached. A network with a high work factor is difficult to break into, while a network with a low work factor can be compromised relatively easily. If hackers determine that your network has a high work factor, which is a benefit of the layered security approach, they are likely to move on and seek other networks that are less secure.

To increase the hacker's work factor, security solutions should be implemented at five key layers of the information network:

1. **Perimeter** – the gateway to the network from the external world. Typically firewall, gateway antivirus, VPN and intrusion detection/prevention systems are placed at this critical point in the network.
2. **Network** – the infrastructure (switches, hubs, routers and wires) that creates the connections from one device to another. At this layer, traffic can be monitored and inspected to ensure no malicious data is "on the wire."
3. **Host** – the computers on the network. Checking for security holes on each machine is imperative. Additionally, mission-critical machines are often monitored for any abnormal changes (using host-based intrusion detection technologies).
4. **Application** – the custom and packaged software that an organization runs in the normal course of business. Protection from flaws in the software is generally accomplished with vulnerability scans, patches, and application shields.
5. **Data** – the actual information stored on the network. Security polices at this layer employ tight access control and encryption.

Once a layered security policy has been created, the focus can turn to implementation. Many healthcare organizations have already implemented basic firewall and antivirus solutions as the core of their network security (implementing the perimeter layer). These measures are an excellent start, but alone they are likely insufficient to achieve HIPAA compliance. Key additional areas that should be considered include access control, monitoring of and response to security attacks, and systematic scanning, testing, and management of security holes.

In an ideal world, healthcare organizations would all have the budget and resources to implement in-depth security measures at all layers outlined above. Unfortunately, we don't live in an ideal world so healthcare organizations need to evaluate their network – how it is used, the nature of the data stored, who requires access, its growth rate, etc. – and then implement a blend of security measures that provides the highest level of protection given the available resources.

Healthcare organizations have long been under scrutiny when it comes to implementing IT policies and procedures but HIPAA has elevated its importance and helped redefine how providers handle patient and financial data. Because of HIPAA, organizations are now open to a range of potentially damaging consequences including fines, liability claims, criminal charges, and even prison terms. Although HIPAA regulations are already in effect, compliance can be achieved over time. The good news is that it can be a

relatively straightforward, cost-effective process when efforts include layered security for the network.

---

**Mitchell Ashley** is chief technology officer and vice president of customer experience at StillSecure, a Louisville, Colo.-based network security provider. He may be reached at [mashley@stillsecure.com](mailto:mashley@stillsecure.com).

--