

# High-Tech Checkup

New technology helps health care providers protect patients' information

As health care organizations implement new technology to improve their efficiency or try to meet the stringent standards of security and patient care mandated in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), their dependence on technology increases exponentially.

That dependence manifests itself in many ways and most health care organizations can become overwhelmed quickly. A 2005 survey on HIPAA compliance by URAC, a Washington D.C.-based nonprofit organization that promotes health care quality through accreditation and certification programs, found that organizations spend far too much money on technology that deals with some issues, but overlook other tools that would have been far more useful.

After reviewing the practices of hundreds of different health care organizations, URAC identified four key problems hurting the ability of organizations to meet HIPAA's security demands:

- » Incomplete or inappropriately scoped risk analysis efforts.
- » Inconsistent and poorly executed risk management strategies.
- » Limited or faulty information systems.
- » Ineffective security, incident reporting and response.

Updated infrastructure can meet many of those demands. Some of the greatest advancements in security, fault tolerance and risk mitigation are commonly found as the core of many new networked systems. Just the simple task of updating your legacy equipment can go a long way toward having the secure compliant organization you seek.

The case study of Yuma Regional Medical Center in Yuma illustrates this point. The main goal was to improve efficiency by updating the network to a more unified platform. The environment at the time was outdated and not up to industry standards. This had created an unstable environment. After the update, YRMC gained the efficiency and stability it needed while also streamlining the IT processes.

**High Availability:** While a simple concept, this is probably one of the most important foundations of any IT infrastructure. Implement a high-availability solution and downtime ceases to be an issue (planned or unplanned). In the event of a disaster — local or global — critical patient information, including insurance information, can be retrieved from a remote location at a moment's notice if planned properly. High-availability historically was a myriad of complex clustered systems and redundant expensive hardware, but with the emergence of virtualized systems technology, high availability can be implemented for a fraction of the cost and capitalizes only a fragment of the IT department's resources, allowing them to become more proactive and less reactive.

**Risk Management:** It may seem like risk management and high availability are one and the same, but a closer look shows that even redundant systems can still be at risk. Viruses, faulty backup solutions, poor access controls and a lack of system policy and procedures can put the infrastructure at risk. Because of the complexity of integrated systems between a varying array of departments and the legal impli-

cations of a lack of policy, the risk analysis process is a company-wide issue, not just an IT issue. Identifying risks and planning policy and procedure protocols should start at the executive level and touch every employee, every department and every corner of the physical infrastructure. Take an active role in identifying key systems, prioritize and plan for typical disasters. Understand that disasters can be man-made, acts of God and even legal in nature. Protect your company's infrastructure, protect your ability to provide patient care and create solid enforceable procedures.

**Internal Controls:** A new infrastructure's worst nightmare is a lack of internal controls. Once you have achieved your IT goals and compliancy is an afterthought, internal controls are the next logical step. These standards and operational best practices provide a framework to start defining your organization's internal controls. These repeatable routines help maintain a healthy network environment and ensure that your network remains vibrant and compliant.

Being compliant with HIPAA has become serious business, but with new technology that road has become a less painful and complicated one to travel. What used to be an overwhelming task for the executive level, delegated to its own internal IT department with hopes that compliancy was achieved, is now a concept grasped by every level of the health care organization. **AB**

*Brian Fisher is a senior systems consultant for BVA Inc., a global technology consulting firm based in Phoenix. For more information, visit [www.bvainc.com](http://www.bvainc.com).*

