

## EHRs and Information Availability: Are You At Risk?

**The EHR initiative is changing the face of disaster and the nature of prevention planning.**

*By Jim Grogan*

On April 27, 2004, the age of the electronic health records (EHR) in the United States took a major step forward. President Bush called for the creation, at the federal level, of a National Coordinator of Healthcare Information Technology within the Department of Health and Human Services (HHS). Today, HHS has appointed the Healthcare Information Technology Standards Panel (HITSP) to coordinate the development of standards, and has awarded contracts to four companies to develop prototypes of a national health information network. The goal for these competing contracts is to see if by using standards-based architectures, information can be effectively shared across what, in essence, will be competing commercial solutions.

Many elements will contribute to the success of national EHR standards, including acceptance by multiple commercial vendors, efficient automated system interfaces to populate the records and maintain data integrity, and support and compliance with all applicable healthcare regulations. When planning for disasters in the age of EHRs, organizations need to consider external and internal authorized users of the electronic health records and their requirements for accessing data. Vigilant security officers and others need to prepare for the very real possibility of unauthorized users breaking into systems and creating havoc. Organizational leaders must realize that EHRs will inevitably fail, and determine how to maintain access to critical data and systems. Finally, organizations must decide how practitioners can provide patient care when the EHR is not available for making clinical decisions.

Reviews of statistics consistently have pointed out that medical practice can be improved by reducing the medical errors that occur during treatment. Errors may be based on incomplete medical records, transcription mistakes, or failure to correlate medical histories with current treatment decisions. The effective use of automation can allow practitioners at every level to make decisions and treat patients to the best of their abilities.

Assuming that broad-based acceptance of national EHR standards occurs in the next eight years, it is reasonable to expect that doctors, nurses and associated practitioners will become dependent



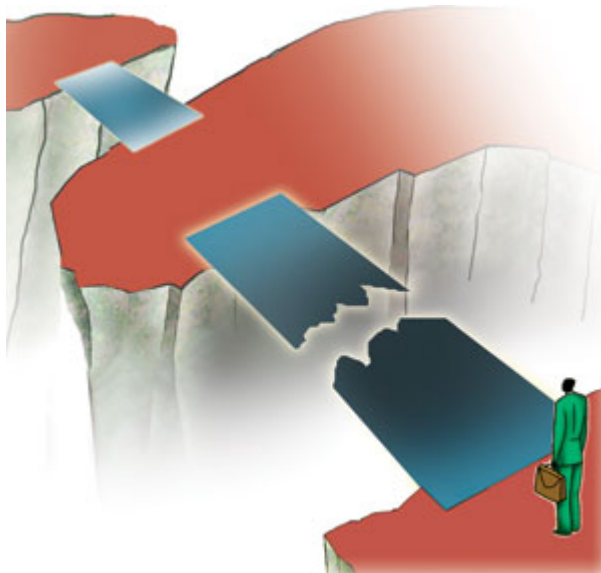
*Jim Grogan is vice president, consulting product development for SunGard Availability Services in Wayne, Pa. Contact him at [jim.grogan@sungard.com](mailto:jim.grogan@sungard.com).*

on automated information. With vast amounts of personally identifiable information in any health record, consumers face risks of abuse or privacy breaches. There are many examples of this today in the frequent theft of individual financial information. EHR data faces the same type of risks; it requires well designed security provisions and constant monitoring of the effectiveness of this electronic security.

### **Accessing EHRs**

Access and information security go hand-in-hand with EHRs. Within the realm of authorized access, solutions need to accommodate both internal and external users of the system. Internal users—institutions, physician practices or healthcare networks—have regular access to patient information in a constant manner as part of the delivery of care. This includes review of current medical histories, drug interactions and allergies, and various departmental studies such as MRIs, CT scans and laboratory results. Authorized external practitioners may from time-to-time require access to studies or other EHR elements.

In developing the standards, the HITSP is preparing “use cases,” which both define and validate the standards with cases that are typical in the practice of medicine. These use cases include clinical vignettes that examine practical access points that are essential to EHR success. EHR value comes from providing rapid access to necessary medical records and departmental results to authorized providers, and an electronic audit trail must be maintained to document the access by each authorized caregiver.



For companies building EHR systems and the institutions that run these systems, access authorization depends on integration with security systems. Individual security authorization systems vary between commercial solutions. One system may be password or smartcard authorized, while another may use biometric identification. To ensure patient privacy, authorized caregivers are only provided access to appropriate information relative to a patient in their care.

Numerous other parties require authorized access, too. These may include insurance companies and payer organizations, drug companies and federal drug regulators, pharmacies and patients themselves.

Organizations or individuals may need to access the EHR for legitimate reasons from outside the original care delivery organization. Because they need to have constant and reliable access to those data and systems, the individuals and organizations become stakeholders in any plan to prevent system failure or disaster.

### **Security of Data and Infrastructure**

Each organization that provides authorized access also must prepare for unauthorized access.

Hackers, and more broadly speaking, data thieves, view the accumulated EHR data as a valuable commodity. Securing the EHR infrastructure is a given; having effective and vigilant monitoring of all access is a responsibility of each organization that houses or owns the electronic data.

Ultimately, the patient is the beneficiary of this information protection, just as citizens count on banks and other financial institutions to protect and keep private sensitive information. As financial institutions have seen, for each electronic fence or border that is constructed, determined individuals and organizations will attempt to breach the security and gather information for malicious intent, or compromise the EHR infrastructure or data to disrupt reliable patient care.

### **Consideration of Failures**

What happens when there is a disaster, failure or interruption within the EHR architecture? We need to immediately consider the impact on the quality of patient care. Automated systems are not new to business models, and we can learn from past experiences outside of the healthcare arena.

A phenomenon surrounds the implementation of any automated support system: During the implementation phase, a degree of trepidation exists among users of the new system based on fear of technology, incomplete or inadequate training, and basic human nature that resists change. After the initial rollout when systems are functioning smoothly—the operational phase—an excitement accompanies the boost in productivity and efficiency, both of which have been mentioned as goals throughout the national EHR discussion over the past several years. After a period of time, however, even the best systems will require and undergo constant refinement and improvements during maintenance phases.

As systems become accepted, the old processes (preautomation) lose ground in corporate memories. Users become dependant on automation to perform even the simplest tasks. Prior to automation, downtime procedures are simple: fall back to manual reports, manual operations, paper records and continue as best as possible until the automated system is restored.

However, highly automated support systems like future EHRs often will lack the paper records needed to fall back on during a system failure or disaster. When it comes to implementing EHR solutions, information resilience cannot be an afterthought, but needs to be designed into the solution at the start. Traditional tape backup or electronic data replication requirements can only be determined by examining the impact on patient care before an outage occurs.

EHR systems make it far easier for users to review the digital information in real-time and to take advantage of automated diagnostic tools that help practitioners to quickly pinpoint irregularities. When planning for disasters or failures, those charged with this responsibility need to consider those who electronically access medical histories and test results and the levels of efficiency, productivity and the quality of patient care they need to provide.

### **Sources of Risk: Disasters and Downtime**

The only prediction that is certain about EHR systems and supporting infrastructure is that they will fail at some point. The best-designed systems are subject to physical threats or electronic

attacks. The highest quality components experience normal wear and tear and either fail or need replacement, introducing downtime. Possible sources of system failures include:

**Natural disasters.** Hurricanes, floods, earthquakes and tornados will continue to cause downtime for operations within their impact area. During natural disasters, the healthcare community often is called upon to join first responders in helping injured people within a region. In addition, stakeholders outside the region may continue to require remote access to EHR information in treating patients.

**Application failures.** For a variety of reasons, software may completely fail or may operate in a degraded mode. Sometimes these failures are defects in code that may have been undiscovered, and more frequently, they are related to transaction volumes that may have outpaced the ability of the software or hardware to meet performance specifications. Volume-related failures could be an issue for Internet-connected applications when there are sudden peaks in workload.

**Infrastructure failures and man-made disasters.** Years of experience have helped companies improve infrastructure. Power systems, cooling systems and data network, however, do experience outages. A comparatively minor traffic accident can bring down utility poles. Fires can disrupt the normal operation of any facility. Intentional malicious actions can force an institution to suspend their normal procedures while law enforcement responds. During such events, it would be commonplace for primary care physicians remote from a centralized facility to continue to treat patients in their offices and to require access to EHR information.

**Security Breaches and Virus Attacks.** The threats are real that individuals or organizations attempt to compromise security procedures. Computer viruses, once found within an institution's systems, are difficult to remove and may require system shutdown to repair damage to critical files and software. Even with careful attention to monitoring security events and utilizing antivirus software and firewalls, new attacks are reported that can take advantage of operating system and application weaknesses. A recent McAfee virus map (February 2006) shows more than 1,000 infected computers per million citizens in North America during a 30-day period.

**Planned Downtime.** Some amount of planned downtime is inevitable to maintain automated systems, while patient care continues 24 hours per day.

### **Impact on Patient Care**

For EHR systems, a critical consideration is how to provide patient care when the EHR—or portions of the data—is unavailable to those who need to make medical decisions. If a clinician must make a decision in an emergency care situation without all the facts, how will this affect the way medicine is practiced? Certain tools can be made available in physical form or perhaps in an “offline” mode. For example, practitioners can rely on reference books if available, but they lose access to automated features that rapidly correlate drug therapies or interactions with a specific patient's existing medications or allergies when electronic systems are down.

The lack of patient-specific physical records during any automation failure will severely impact a practitioner's ability to deliver high quality care. Many procedures require the physician to consult radiological studies during the procedure. The absence of this capability to check the

studies mid-procedure changes how a physician or surgeon may need to complete the procedure. Many treatments involve frequent monitoring of laboratory results to adjust medication levels, something that is hindered if the automated systems are unavailable.

### **Stakeholders**

In the evolving world of electronic health records and electronic medical records, it is best to prepare for automation failures by considering the various stakeholders depending on the timely, accurate availability of patient information. These include:

- The patient;
- Primary care physicians and staff;
- Attending physicians and nursing staff within a hospital or institution;
- Specialist care providers—both within and outside the facility where the patient is being treated;
- Ancillary department medical staff;
- Insurance providers;
- Pharmacy staff;
- Outpatient healthcare facilities;
- Home healthcare and hospice professionals.

With each stakeholder, it is important for individuals within organizations to discuss information that might be missing during an automation outage and to develop appropriate protocols for delivering treatment. Staff involved on these protocols need to be trained, and the training must be updated on a periodic basis.

### **Increased Dependence on Automation**

Healthcare delivery is becoming dependent on information technology, as evidenced by the increased use of automation in all aspects of patient care—from computer aided diagnosis, drug interaction, image-guided surgery and physician order entry. The EHR, coupled with the widespread deployment of a national health information network in the future, will increase this dependence on patient information being available in real-time to clinical practitioners. Many traditional components come into play to help those utilizing EHRs keep connected to the data and systems they require. These include provisions for effective electronic security and privacy controls, high availability data protection architectures, and cost-effective recovery of operations from any disruption.

Downtime procedures and carefully planned medical treatment protocols to be followed during automation failures are essential. When intraoperative computerized tomography is used in the surgical suite, there must be contingency plans if the failure occurs before or after surgery begins. Similar considerations are needed for interventional radiology and other areas of modern healthcare delivery.

As the nation prepares for EHRs and a national health information network, private and public sector groups will continue working together to adopt standards that meet the goals of improved patient care. Each stakeholder needs to be considered under the magnifying glass of information availability—the real-time access to information by healthcare providers around the clock.

Each stakeholder, too, has an obligation to consider how inevitable outages can be mitigated through carefully designed downtime procedures and supported by established medical protocols. The future is evolving at a fast pace for the healthcare use of automation, and there are no signs of this slowing down. Each vendor and practitioner needs to build in the protection that will be a key to the success of this immense project.

For more on **information availability services from SunGard Availability Services**,  
[www.rsleads.com/605ht-201](http://www.rsleads.com/605ht-201)

© 2006 Nelson Publishing, Inc