BEHAVIORALHEALTHCARE

Issue Date: January 2009

Data at rest = data at risk

A provider strives to improve data security while transitioning to an EMR

by Steven Porter

Security is a journey, not a destination.

I'm not sure when I first heard this adage, but it never had been more apparent than following Touchstone Behavioral Health's (TBH) initial deployment of a hosted electronic medical record (EMR) system for our highly mobile staff. Due diligence led us to a HIPAA-compliant application with role-based accessibility. We spent months honing policies, fine-tuning procedures, and implementing advanced technologies to secure both our network and individual computers. Training and awareness programs educated users about viruses and worms. Phase one concluded as a major success: We effectively gathered and reviewed confidential client information, securely transferring it to and from our remote data center while providing services out in the community. Although our data “in transit” were protected, we realized that work still needed to be done with our data “at rest”—information stored on local hard drives and removable media.

Creating a secure infrastructure

TBH provides evidence-based outpatient services to Medicaid-eligible children in Arizona. Our model is to meet clients and their families wherever they are most comfortable. Although we support five clinical locations across the state, the majority of our encounters are in homes, schools, or other community locales.

We chose an EMR system from Credible Behavioral Healthcare Software, and it meets all of our primary application requirements: ease of use, intake-to-billing integration, and hierarchical role-based security with full reporting to support our “anywhere, anytime” care philosophy. This software-as-a-service (SaaS) solution enforces strong password authentication and encrypts bidirectional data transmission between us and the vendor's hosted data center.

Between May and June 2007, TBH obtained, configured, and deployed approximately 120 Dell Latitude laptops in preparation for the EMR launch on July 1. To provide enterprise-level security for all of our computers, with minimal end-user impact, we chose Symantec Endpoint Protection, which offers an integrated personal firewall, advanced antivirus and antispam engines, and a “behavior-based zero-day threat mitigation” application (Traditional antivirus solutions look for specific blocks of code or “signatures” within potential “malware” [change the signature and the code slips through]. Behavior-based systems examine the code's *intent* and block unexpected activities from executing). Combined with our existing traditional network defenses (intrusion detection and prevention, firewalls, application patching, content filtering, and e-mail encryption) and the EMR vendor's secure Web-enabled capabilities, we confidently transitioned from a paper-based system into an exciting new era leveraging technology to support our care model.

In January 2008, we began our review of phase one, and the results were very gratifying:

- User acceptance was nearly universal (Some always will be more resistant to change than others).
- Workflows were streamlined, eliminating redundant steps in the documentation and billing process.
- Contract compliance was improved as TBH's business rules were encapsulated within the EMR to provide proper account coding.
- Per-provider billing was improved by approximately 5%, despite the new system's learning curve and a change of our major regional behavioral health authority midway through the six-month transition.

More importantly, we successfully initiated a culture of data security, merging technology, policy, and user awareness to minimize our risk of a data breach.

This analysis also focused on where data reside within our systems, and how they are protected. We reexamined role assignments within the EMR system to ensure that each provider had access only to information necessary to complete his/her assignments, and that strong password authentication was functioning properly. We reviewed our database audit capabilities, as well as our internal network security policies and procedures. Finally, we looked at our users, the equipment they carry into the field, and the data they need to provide services. We concluded that the biggest remaining vulnerability was with physical devices (laptops, flash drives, CD-ROMs) and the information stored locally.

Protecting locally stored data

Major data loses regularly make headlines. News reports frequently discuss stolen or misplaced devices, such as missing hard drives at a national research lab, a stolen VA database administrator's laptop, and backup tapes lost during shipment to an off-site location. High-profile breaches are common, but thousands more losses every year never are reported in the general press. Devices are stolen from cars and homes, and computers are left in coffee shops, hotel lobbies, taxis, and airports.

Nominal security policies requiring strong passwords and an enforced lockout period after a few failed log-in attempts are enough to discourage the casual “finder” (It's easy enough to sell the device for a few dollars or simply reformat the drive for personal use). Our real concern are dedicated data thieves, those technically savvy enough to bypass our first line of defense and access the device's contents. To these individuals (and, increasingly, criminal organizations), the real prize is not the device but the information it contains. Thus, phase two of our technology evolution was to further secure sensitive data, regardless of their location.

What we were looking for. In March 2008, we began defining the ideal features of a more secure system. At the top of every list was end-user transparency. Our solution had to work with minimal user intervention and as unobtrusively as possible. Also ranking high was the need to be “device agnostic.” We required data protection on any device—a laptop, thumb drive, CD, etc.

The third component was data portability (the capacity for authorized users to access stored data wherever they need them regardless of the device used) and that data could be recovered at an administrative level. We wanted our data to remain protected even if the storage medium were separated from its associated device (e.g., if a hard drive was connected to another system, the information would remain secure).

We also required granular administrative control from a centralized console. That is, we needed the ability to define security policy and access rules across the network, even if the machine is physically at a remote clinic. We wanted the system to enforce “phone home” capabilities, so that computers regularly would verify authorization against a master list and deny access if the machine has been compromised. Finally, we wanted a method of signaling a device's physical location to facilitate asset recovery when, not if, a machine disappears.

What's available. A surprising number of solutions offering two types of security are available.

Asset recovery offers a certain sense of satisfaction—knowing the perpetrator (or some poor sap who thought he was getting a great deal) will be caught and punished for taking the hardware. The recovery intelligence usually is tied directly to the computer's motherboard: Every time the machine boots it checks for an Internet connection and, if present, contacts a remote database. A machine reported missing halts the boot process and, in some cases, sends its IP address to the authorities. This is a great offering for organizations using high-end portable workstations in which the hardware itself is of great value. Unfortunately, asset recovery generally doesn't prevent someone from moving the hard drive to a second machine to recover the data, as asset-recovery software works only on devices in which it's installed.

Encryption is designed to secure data and comes in a variety of flavors. *Full disk encryption* is readily affordable (it's often packaged with premium operating systems and on many business-class computers). Everything is secured, but there are significant drawbacks from both administrative and user perspectives. Each machine will need an admin password to ensure data recovery as well as a unique user password for daily operation. Without a central console, admin passwords must be changed at each individual machine. Users have access only to specific hardware, adding overhead to routine maintenance and equipment life cycles. Users must remember a machine-specific password in addition to their network credentials.

Also, with full disk encryption, everything on the disk goes through the same encryption process, including the operating system and application files. Before the machine can perform any function (e.g., launch Word) it must first decrypt the basic program software, then the file a user is attempting to open. Full disk encryption, by design, will slow computer operations because of the additional processing required.

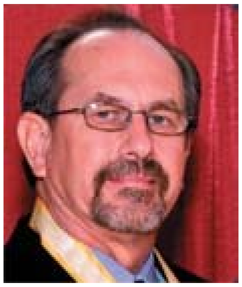
File-level encryption also offers a couple of options, but generally reduces complexity for the end user. Some systems simply encrypt anything stored in a particular location. For example, an administrator designates the “My Documents” directory or creates a “Secure” folder on each machine, and users store sensitive files in the proper areas.

File-type encryption is another option. An administrator specifies that all files created with specific applications (e.g., Microsoft Word, Excel, or PowerPoint) are encrypted wherever they're stored. This ensures that data are secure *unless the user specifically modifies the file extension* (e.g., changing .xls to .old, then moving the file to another machine, and finally changing the extension back to .xls). This is an important distinction, as such a system can be deliberately defeated.

What we chose. We selected CREDANT Mobile Guardian to encrypt our data “at rest.” It has a data-centric approach to security. In addition to looking at file extensions, the solution examines the data within the file (e.g., verifying text is indeed text, numbers are numbers) regardless of what the file is named. The product doesn't care where the data are stored: Removable devices like thumb drives are no longer the weak point in a secure architecture. The central administration console provides the granularity we require and integrates with Microsoft's Active Directory so that data are available anywhere with appropriate network credentials (and can be recovered at the admin level). Asset recovery is not included at this time but could be rolled into a future release.

Final thoughts

TBH's mission is to work with children experiencing difficult times and to help them attain the skills necessary to live productive and responsible lives. Technology is one of the tools we use to increase our own productivity, allowing us to spend more time with our clients. Ultimately, data security is just a part of the service we provide.



Steven Porter is CIO of Touchstone Behavioral Health of Glendale, Arizona.

Touchstone Behavioral Health, based in Glendale, Arizona, provides positive outcome, evidence-based behavioral health services to youths and their families through prevention and outpatient therapy. Founded in 1968, TBH has five offices throughout Arizona. The agency was recognized in 2008 as a Computerworld Honors Program Laureate for the project “Secure EMR for Remote Providers.” For more information, visit http://www.cwhonors.org/viewCaseStudy2008.asp?NominationID=764 or e-mail steven.porter@touchstonebh.org.

Sidebar

touchstone
behavioral health

- Serves Medicaid-eligible children in Arizona
- In FY 2008 served 3,845 juveniles
- 175 staff members
- $10 M budget (FY 2008)

Behavioral Healthcare 2009 January;29(1):24-26