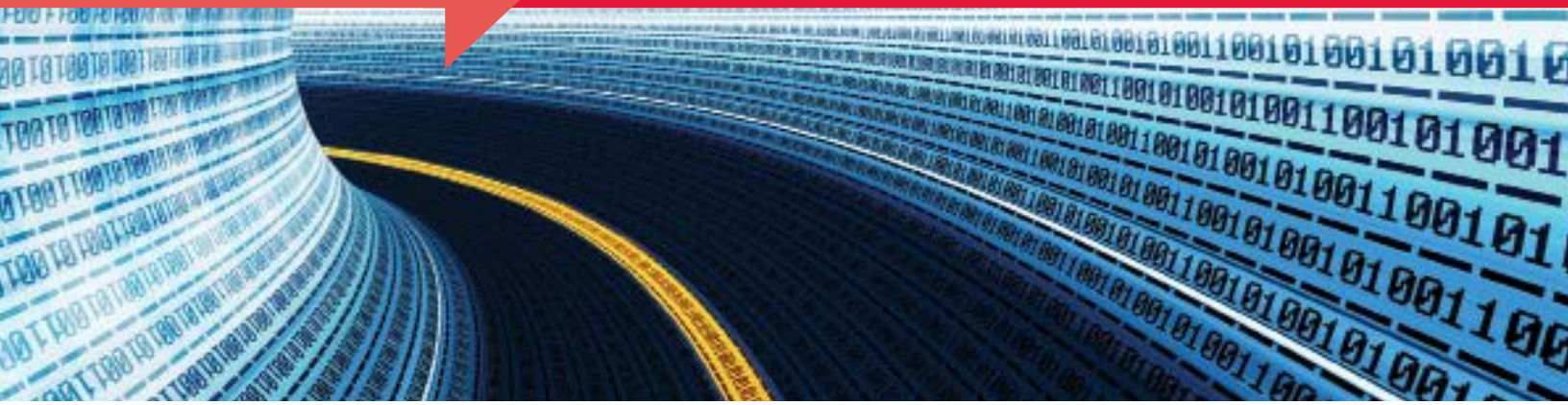
TOP 10

TOP10 BEST PRACTICES FOR SECURING HEALTHCARE DATA BEFORE MIGRATION



Introduction Merger and acquisition activity in healthcare continues to trend upward. Some of the main reasons for this growing trend include hospitals looking to acquire physician practices in an effort to align providers with organizational goals; the outpatient industry progresses in response to demand for lower cost care; and healthcare regulations and reimbursement cuts compel smaller providers to seek growth through alliances with larger organizations. Hospitals and doctors are also adopting digital records to qualify for federal incentives that are meant to slow rising costs, reduce duplicate tests and reduce human error.

However, migrating patient data from paper-based records to electronic records or merging electronic databases is complicated – and there's no room for error. Electronic data must first be standardized and then stored on compliant systems that are secure but accessible, and affordable but always available. If you're a CIO or IT manager facing the gauntlet of migration, here are the top 10 best practices for securing healthcare data before you start:

#1. Assess the financial impact

Data standardization costs

Before data from paper-based records or different systems can be migrated or merged, it must be standardized so that terminology is consistent across records and offices. Standardizing data requires either manual coding or the purchase of software that automates the process, or a combination of the two. Manual coding can be expensive: You'll need extra staff or specialists to go through all patient records, and you'll have to accept a fair amount of lost productivity and downtime for content freezes before and during migration.

Software that automates the process may turn out to be less expensive and more accurate, but it still requires an investment and attention from staff.

Storage, hardware and infrastructure costs

The International Healthcare Data Management Survey [1] reported that digital storage of medical images such as X-rays, MRIs and ultrasounds are responsible for explosive data growth in the healthcare industry. In fact, 46 percent of respondents in a 2011 survey reported a 25 percent to 50 percent increase in data over the previous year. [2] As technology improves, plan for data to continue to grow at this rate or higher for the foreseeable future.

[1] BRIDGEHEAD SOFTWARE 2011 INTERNATIONAL HEALTHCARE DATA MANAGEMENT SURVEY

[2] COMPTIA THIRD ANNUAL HEALTHCARE IT INSIGHTS AND OPPORTUNITIES, 2011

TechTarget Custom Media

CDW PEOPLE WHO GET IT™ HEALTHCARE

Undoubtedly, a comprehensive storage strategy is requisite for mergers, and a long-term view can save thousands of dollars down the road. Increased storage in a physical data center requires an investment in additional hardware and infrastructure, while cloud-based storage may cost less but still require you to upgrade high-speed connections.

Software licenses

If you're merging practices, plan for a significant software expense in the form of standardized practice management systems (PMS). When evaluating practice management software, find out if licenses are required for each user and how part-time staff is counted. And, though it may be tempting to take advantage of bulk discounts, beware of vendor lock-in. If all of your software (and hardware) comes from one vendor, you're at the mercy of its design and stability. In the end, vendor lock-in can end up costing you any savings you realize from a bulk discount.

Lost revenue from downtime

Because no amount of testing can uncover every possible problem, make room for some measure of revenue loss associated with potential downtime during the launch. CFOs should understand what each hour of downtime costs their organization, and there are many online calculators that can help you make an educated guess. A simple starting point is to add your employee costs per hour to your average income per hour. [3]

Security monitoring

Ponemon Institute's Second Annual Benchmark Study on Patient Privacy and Data Security concluded that "data breaches in healthcare organizations are rising more than 30% year over year, with most organizations stating they've been breached in the past year." [4] Even one data breach incident can cost an organization thousands of dollars in fines and the loss of consumer confidence. Large organizations, especially those that are regulated, must plan for additional costs associated with increased IT staff or a third-party security monitoring service.

#2. Ensure compliance

Regulations that govern how patient records and payments for services are handled multiply every year – as do the fines for not following the rules. Among the most critical healthcare and electronic medical record (EMR) and electronic health record (EHR) [5] regulations are:

- HIPAA: The Health Insurance Portability and Accountability Act was enacted to protect patient privacy.
- SOX: The Sarbanes-Oxley Act sets standards for corporate accounting and responsibility.
- PCI DSS: The Payment Card Industry Data Security Standard ensures any organization that processes, stores or transmits credit card information maintains a secure environment.
- HITECH: The Health Information Technology for Economic and Clinical Health Act, part of the American Recovery and Reinvestment Act of 2009, mandates implementation of EMR/EHR systems by 2014.

While none of these regulations spells out the exact functional requirements for hardware, software, storage or

3 A SIMPLE WAY TO ESTIMATE THE COST OF DOWNTIME, DAVID A. PATTERSON, COMPUTER SCIENCE DIVISION, UNIVERSITY OF CALIFORNIA, BERKELEY

4 SECOND ANNUAL BENCHMARK STUDY ON PATIENT PRIVACY AND DATA SECURITY, PONEMON INSTITUTE, 2011

5 NOTE: EMR REFERS TO ELECTRONIC MEDICAL RECORDS OWNED, MANAGED AND CONTROLLED BY A PRIVATE PRACTICE PHYSICIAN, WHILE EHR REFERS TO ELECTRONIC HEALTH RECORDS THAT SPAN TIME AND MULTIPLE PROVIDERS AND INSTITUTIONS.

security, they determine the minimum standards for the final results of the entire data environment. You must ensure that any infrastructure you implement meets compliance regulations – and beware taking a vendor's word for it without having it guaranteed in a contract. If you encounter a violation, you'll be the one paying the fine.

#3. Plan appropriate storage

Physical storage security

A consolidated data storage plan for branch offices eliminates the need for individual branch office staff to perform security, maintenance and backup tasks. Whether you choose a physical data center with virtual servers or cloud-based storage, compliance regulations mandate that your storage is secure. Data centers should be unmarked buildings with limited entry points, and they should not be located in geographical high-risk areas. Data centers should also have redundant power supplies and the appropriate architectural security and fire protection.

Cloud storage security

The security and reliability of cloud-based storage is still hotly debated, but more and more large enterprises are using cloud storage, especially for noncritical data. One of the major perks of cloud storage is that storage space can scale on a "pay for what you use" basis with no manual intervention.

Either way, you should ensure that you can buy the right amount of storage for today and add to it as needed. Over-buying storage in anticipation of growth doesn't actually solve or prevent storage problems in the future; it only takes money out of the budget that could be used for today's needs.

#4. Plan backup and high-availability strategy

High availability for productivity and audit response

Whether you're backing up data to a physical data center or in the cloud, your data must be consistently accessible. Most regulations have requirements regarding the availability of records for audit purposes, and there are hefty fines if you can't produce them in time. Cloud storage has had availability problems in the past, but a physical data center isn't completely foolproof either. Carefully evaluate the availability risks of both for your situation.

Get the data out of the building

Third-party software that replicates data and applications in real time to a redundant server is a trusted method for disaster preparedness and recovery. Software that is hardware-agnostic (doesn't require the exact same make and model of redundant server as the production server) can save time and money in the event of a disaster. Optimally the co-location should be at least a ZIP code away from the production server, but an even better strategy to prevent downtime from regional disasters is to situate it in a different time zone.

Triage data

Keep in mind that it's not necessary that all data be backed up in the same way. Lower priority data and data that is not private or sensitive doesn't have to be backed up in real time or immediately retrievable after a disaster or system outage. Triaging data can save time and money.

Test regularly

Remember to test your backup system regularly – don't wait for a disaster or widespread outage to find out if everything is still working.

#5. Standardize data

Standardizing data means establishing consistent technical terms and methods of documentation across organizations. There are infinite permutations of natural shorthand and regional vernacular, which vary from practice to practice, and each practice will have established its own method of documentation before a merger. When it comes to the standardization process, you have options:

- The vendor that provides your practice management software may offer a conversion service.
- You can hire consultants who specialize in migrations to do it manually.
- You can use third-party software that maps and matches terms.

Manual coding can be extremely time consuming and therefore expensive, and it can yield low-quality results. Because healthcare data conversion and mergers aren't new territory, the software that exists to automate the process is fairly mature and easy to use. Automated integration software can also prevent the content freezes that bring expensive downtime.

#6. Secure the data

A recent Data Breach Investigations Report revealed that most data breaches could be avoided with simple or intermediate security controls.[6] Before migrating, take time to establish a formal data protection strategy, and determine who will monitor the network for potential risks or breaches. Also, be sure that your technology allows role-based security – you'll need to establish who should have access to what data and establish a regular audit process. The good news is that both of these measures can easily be automated.

Security as a service

Security as a service (SaaS) is an enticing option for large organizations that require continuous, advanced security. After all, why invest in security hardware, staff and software that requires constant monitoring, maintenance and upgrading if someone else can do it for you? SaaS usually comes with a team of IT, security and legal experts who constantly follow your network traffic and alert you of potential problems. One of the most important benefits of SaaS, especially for CIOs, is that instead of security being a capital expenditure, it becomes an operational expenditure. Since you don't own any of the hardware, software or infrastructure, nothing depreciates or falls into obsolescence, and there's no training or license expenses.

#7. Ensure integration with EMR/EHR software

The American Medical Association (AMA) also encourages physicians to adopt EHRs so they can enter the widening circle of physicians who are able to communicate with each other. If you have a PMS or are evaluating one, ensure that it can integrate with EHR systems and exchange insurance, demographic, coding and billing information. The AMA advises that it can sometimes be more cost effective to replace an existing PMS with an integrated PMS/EHR system, as integration costs can be significant. [7]

6 VERIZON WIRELESS 2012 DATA BREACH INVESTIGATIONS REPORT

7 AMERICAN MEDICAL ASSOCIATION RESOURCES: ELECTRONIC MEDICAL RECORDS/ELECTRONIC HEALTH RECORDS

Questions to ask your PMS/EHR/EMS vendor include:

- Can the system interface with medical devices?
- Who provides support, and what is the response time?
- Will the software comply with all federal and state mandates?
- Does the vendor guarantee that its software can submit and receive HIPAA standard transactions?
- Does the vendor have a legal license to essential code sets, such as the AMA Current Procedural Terminology (CPT®) file?
- What is the vendor's training approach?
- Does it provide SaaS security and storage service?

#8. Leverage mobility

Entering or retrieving information from a Mobile device allows an EHR system to become mobile, saving time and money.

Native apps

Designed especially for tablets, native apps have fewer technical difficulties, and because they don't interact with Web browsers, they're more secure (provided they require log-in credentials). However, if a tablet with an EHR app is lost or stolen, log-in credentials could be compromised and patient data could be changed or shared.

Browser-based apps

Web browser-based apps can be accessed remotely, giving providers constant access to their patients' health records. However, if log-in credentials are compromised, EHRs could be accessed by anyone.

Special hardware requirements

CompTIA reports that 41 percent of healthcare providers currently use or plan to use tablets in their practice within 12 months.[8] Portable devices used in healthcare practices really have to measure up: They must be lightweight, reliable, waterproof and durable, and they must have a long battery life and extra security measures.

#9. Plan access management

Role-based security

As for role-based security, your protection plan should include identity and access management software that manages passwords, provides role-based access and automates audits and monitoring. Identity and access management software saves money by cutting down on help desk calls to reset passwords, and it can manage and deactivate user accounts – all with an audit trail for compliance.

Determine BYOD guidelines

CompTIA reports that one in three healthcare providers uses a smartphone or tablet to access EMR/EMH systems.[9] The consumerization of technology means "bring your own device" (BYOD) is a real security concern for healthcare providers. Nearly all employees have smartphones or tablets – and they're bringing them to work.

8 COMPTIA INFOGRAPHIC
9 COMPTIA INFOGRAPHIC

Establish and clearly communicate BYOD guidelines for phones, tablets and flash memory drives in provider facilities. You also need to ensure that your security monitoring procedures or service allows employees to consolidate to one device while allowing you to maintain control over sensitive data.

Remote access guidelines

Safe remote access to EHRs requires a Secure Sockets Layer virtual private network connection, a firewall on the network, an audit trail and role-based access controls. Additional precautions are time-out parameters, antivirus software, data encryption and download prevention. Even with this framework in place, healthcare providers should approach remote access with caution: It should be limited to critical situations, and CIOs must be prepared to document how they protect patient data.

#10. Make a go-live plan

Full migrations

Many organizations have the luxury of weekend migrations: If something goes wrong the IT team has an opportunity to work it out before customers and employees expect service on Monday morning. If the provider is closed on weekends, a one-time, full migration avoids synchronization issues and minimizes downtime risk.

Incremental migrations

However, if the organization runs 24 hours a day, seven days a week, migrating in increments (starting with the least-critical business function) or performing a parallel migration may be more ideal. Incremental migrations allow the IT team to perform trials by migrating small subsets of noncritical data first. If bugs are found, they can roll back to the original state or work out problems with lower risk to productivity.

Parallel migrations

A parallel migration ensures that data on the current production system and the target system are constantly synched. If a problem is encountered on the target system during a full or incremental migration, users can be directed to the legacy system while the problem is solved.

Preflight testing

In any scenario, preflight testing should cover functionality, access and security, followed by backup and recovery system testing. It's imperative that no data is lost during downtime, so users should always have access to a stable system (if they are permitted access at all) during the migration.

Conclusion

Healthcare mergers and consolidations as well as government mandates are driving hospitals and doctors to adopt EHRs and documentation practices. While electronic records benefit the patient and the provider by lowering costs and increasing efficiencies, migrating from paper records or merging electronic data from multiple sources can be extremely complex and pose significant risk to the practice. Careful planning can help keep sensitive data secure during migration and reduce costs and risks for the organization.

TOP 10 TOP10 BEST PRACTICES FOR SECURING HEALTHCARE DATA BEFORE MIGRATION

This paper is sponsored by CDW Healthcare, a leading provider of technology solutions and services focused exclusively on the healthcare marketplace. Our customers include more than 15,000 healthcare organizations nationwide, ranging from small physician practices to large hospital systems. At CDW Healthcare, we have the knowledge and expertise to understand your IT infrastructure and deliver the broadest choice of solutions. Visit CDW Healthcare at ***www.cdwcommunit.com.***