DATA PROTECTION STRATEGIES FOR THE HEALTH IT PRO

Protecting patient data should be a major concern for health care organizations of all sizes. Encryption technology, strategically used throughout an organization, can prevent data from falling into the wrong hands.

- USE RISK ANALYSIS TO IDENTIFY DATA ENCRYPTION NEEDS
- KEEPING UNENCRYPTED PATIENT DATA OUT OF BACKUP TAPES
- WITH DATA SO VULNERABLE AT REST, HARDWARE ENCRYPTION A MUST
OUNCE OF ENCRYPTION, POUND OF CURE

Encryption technology can save health care professionals from being the victim of, and having to report, a data breach.

BY BRIAN EASTWOOD

DATA—PARDON THE PUN—is the lifeblood of the modern health care industry. It helps physicians make treatment decisions, it helps patients improve their own health, and it helps providers make business decisions. Data also makes health care organizations a prime target for thieves, whether they want credit card numbers, Social Security numbers or other personal health information.

Unfortunately, health care hasn’t had the best reputation when it comes to patient data security. Since 2009, nearly 400 data breaches, affecting close to 20 million Americans, have been reported to the federal government.

Many of these breaches could have been prevented. Under federal rules, if data is lost or stolen, but it has been encrypted, then the incident is not considered a data breach. This applies not just to data but also to hardware—laptops, thumb drives, databases, backup tapes and so on.

The law does not explicitly tell health care organizations or their business associates what to encrypt or how to encrypt it. Nor do any rules specifically require encryption—they merely note that it is a best practice.

This e-zine takes the next step and provides tips for health IT leaders who are considering data, hardware, network and backup tape encryption technologies for their organizations. If your questions remain unanswered, email me at beastwood@techtarget.com or visit our Health IT Exchange community site to ask your question to health IT experts and peers.

Brian Eastwood is site editor for SearchHealthIT.com.
USE RISK ANALYSIS TO IDENTIFY DATA ENCRYPTION NEEDS

Before deploying data encryption technology, health care organizations should conduct a risk analysis to determine what protected health information they possess and where it is most vulnerable. By Ali Pabrai

**Encryption Is** increasingly a security mandate, not just in federal regulations, but also state regulations, specifically those tied to breach notifications. Federal and state regulations are increasingly emphasizing encryption capabilities, especially for sensitive client-customer or patient information.

For example, your organization may come into contact with what is referred to in these regulations as personally identifiable information (PII). Industry-specific regulations such as HIPAA refer to protected health information (PHI). Whatever the data is called, encryption becomes important because it does in fact allow an organization to protect and secure all sensitive customer information.

**Risk Analysis Can Determine Encryption Needs**

Organizations need to determine when they would encrypt this type of information and, then, on what systems would that information be encrypted. In order for an organization to make this determination, a comprehensive risk analysis exercise must be complete. Many of these regulations, for example, mandate that an organization complete a risk analysis exercise at a certain fre-
Use risk analysis to identify data encryption needs

With data so vulnerable at rest, hardware encryption a must

Keeping unencrypted patient data out of backup tapes

Editor’s Letter

Use Risk Analysis to Identify Data Encryption Needs

Use risk analysis to identify data encryption needs. You may do it once a year or once every 18 months, depending on the regulations that impacts your organization.

This risk analysis activity gives insight into what areas of your enterprise contain the information that would potentially need to be encrypted. When you look at business considerations, and when you look at the workflow in terms of how information moves across the enterprise from a business process perspective, you’re going to be looking at the information in terms of data at rest as well as data in motion.

An example of data at rest would be data stored on a database server, laptop or, increasingly, on the hard drive of an iPad or other tablet devices. On the other hand, when an individual is accessing information from home or when they are travelling, or when clinical applications are participating in data exchange, that is data in motion.

Based on your risk analysis activity, you would then make a determination—what are the areas of your enterprise architecture where you need to encrypt the information? It is becoming increasingly important, especially when you look at compliance requirements, for the information that is being transmitted—data in motion—to be encrypted.

In this case, look at Secure Socket Layer (SSL) and virtual private network (VPN) implementation wherever possible. This way, encryption capabilities will be automatically enabled when information is in fact being moved from one point of the infrastructure to another. This becomes especially critical when transmitting information over an open public network—for example, the Internet.

Another place where organizations must be really sensitive when it comes to encryption in transmission is over wireless networks, as hackers are increasingly able to compromise wireless infrastructure security. Here encryption is not enough. Make sure you have the appropriate encryption algorithm with the appropriate encryption key-bit strength enabled across your wireless infrastructure, as well as when you are moving information across the Internet.

Counting the costs of encryption

The issue of cost frequently comes up when CIOs, executives and other individuals look at encryption. In particular, questions arise about the up-front cost of implementation, as well as ongoing costs related to management and maintenance. Those are very good questions.

The cost component piece of it is generally impacted in three particular areas:

1. The cost component piece of it is generally impacted in three particular areas:
1. One is the **ACQUISITION COST** to acquire the technology and controls needed to implement encryption capability. One example is email. Obviously, all organizations use email. Any email may include attached files that could have customer or client information. One thing to consider is a software tool that will scan all email that is transmitted outside the enterprise and look for keywords such as Social Security Number, credit card number or debit card number. When the scanner finds such keywords in an email, the email is then encrypted as it is released outside the firewall as it gets transmitted. The acquisition of technology such as this is typically done on a per-user basis, so this is an acquisition cost that IT departments will have to plan accordingly.

2. Tied into that is **MAINTENANCE COST**. From my experience, that is about 20% of the acquisition cost, only it will be paid on an ongoing basis.

3. The third element that impacts the cost is the **HUMAN COST**. Encryption does require specialized skills—not just anyone in IT can support it. Make sure that you have either the appropriate security professionals on your team or consultants available on demand that can provide support as needed, both to implement and maintain encryption architecture.

**USE ENCRYPTION POLICY TO DEFINE TECHNOLOGY NEEDS**

Before investing in encryption technology, though, it is really important for organizations to take a step back and focus on two things.

Before determining what kind of solution or controls are needed to enable encryption, conduct a comprehensive risk analysis exercise to understand the risks associated with the sensitive information your organization comes into contact with. Simply put, you have to do this, and there are no shortcuts.

Once that risk analysis exercise is complete, develop a specific encryption policy that is no longer than two to three pages. In your encryption policy, spell out what you need to enable encryption, from a compliance perspective as well as a risk management perspective. For example, your policy could require that all emails containing confidential client information or other types of PII will be automatically encrypted. Make sure the policy provides a foundation for your organization to take the next logical step, which is the acquisition and implementation of encryption capabilities.

Ali Pabrai is CEO and co-founder of the HIPAA Academy.
Use risk analysis to identify data encryption needs. With data so vulnerable at rest, hardware encryption is a must. Keeping unencrypted patient data out of backup tapes.

THE ABILITY TO keep your data protected is becoming more prominent with every passing day. There are a variety of ways to secure data, either on the perimeter or in within the local area network, but the most fundamental method in a defense-in-depth model is encryption at the hardware level.

Data needs to be protected from malicious intent or user oversight. At the basic level of security is encryption or the ability to obscure and render data useless without the proper key. Encryption has been around for quite some time, but its benefits are still not being used to their full potential in the enterprise—and the health care industry is no exception. Encryption at the hardware layer is expected to grow in the future. We tend to focus our protection efforts at the perimeter when, in fact, data is most vulnerable at rest.

In today’s mobile generation, meanwhile, the ability to protect data that’s physically outside your perimeter is becoming an issue that encryption is handling well. The ability to render stolen or lost data useless is an important aspect in securing your information. Encryption at this level is one of the basic building blocks of a secure information security program. Device encryption is one of several hardware encryption techniques that will be described in this article.
FULL-DISK ENCRYPTION BEST FOR LAPTOPS
Laptops represent one of the areas where encryption should be used from a hardware perspective. Laptops can store large amounts of data, and they will most likely leave the building, so your data is at risk if it’s not encrypted.

There are certain methods to perform encryption on laptops, mainly full- and partial-disk encryption. Full-disk encryption encrypts the entire disk, leaving nothing to chance. When logging into the laptop, users are prompted to enter the decryption password before even booting into the operating system. The partial disk encryption method, on the other hand, consists of selecting folders or partitions within the operating system that you deem to be encrypted. This method is quicker but leaves room for more risk if a laptop is lost or stolen, since you can’t guarantee that all the data is encrypted.

When it comes to protecting data on laptops with encryption, full disk encryption is the preferred method. There are many free solutions that can perform encryption within the operating system, such as the open-source TrueCrypt. Others are paid, including CheckPoint Software Technologies Ltd.’s PointSec. Some, such as Microsoft’s Bit Locker, come built into the Windows operating system.

If a laptop is lost or stolen you can replace the hardware, but the data is irreplaceable. Data breaches can harm an organization’s reputation, increase its risk of exposure and subject it to regulatory infractions. In fact, HIPAA doesn’t require health care organizations to report stolen or lost laptops if they have been encrypted. With this being said, full disk encryption should be placed on laptops to protect your data from being lost or stolen in the event that data is removed from your organization.

MOBILE DEVICE MANAGEMENT NEEDS THIRD-PARTY TOOLS
Mobile devices are infiltrating the workplace. IT leaders need the ability to secure the data on them. Like laptops, these devices can take large amounts of data on them outside the walls of your organization. Having the ability to control where the corporate data is, and to ensure that it is encrypted, is a concern for health care providers and companies in general.

With the upsurge of smartphones and tablets in the enterprise, many employees are requesting to use their own devices. While devices can improve productivity, IT departments need to verify that they can encrypt the data on these devices before the business puts itself at risk.

In addition to encrypting the data, it’s also necessary to be able to manage...
MEANWHILE, NETWORK ENCRYPTION WILL PROTECT DATA IN TRANSIT

BY AL GALLANT

To prevent unauthorized server access, a health care institution should encrypt its entire network, both wired and wireless. Network encryption ensures that hackers attempting “sniffing attacks” will not see any protected health information (PHI) in transmission.

By definition, network encryption is applied to the network transfer layer—that is, above the data link level, but below the application level. Using the existing network services and application software, network encryption is invisible to the end user and operates independently of any other encryption processes used.

The following network encryption basics will help health care organizations protect data:

• Be sure the routing works before you try to do encryption. A remote peer may not have a route for the interface, which means you will not be able to have an encryption session with that peer.

• Encrypt your network at the endpoints. Encrypting routers redundantly (decrypting and re-encrypting all traffic) really just wastes CPU cycles.

• Pay attention to network bottlenecks. Low-end routers should not be used in main network cores. You will get a “CPU hog”-type message, because the volume of traffic uses all the router’s CPU cycles to encrypt the traffic.

• If you need to encrypt other than IP traffic, use a tunnel.

• Remember that network encryption applies only to the data in transmission. The data does not stay encrypted when it lands at the destination. If the destination server is breached, that data gets stolen, and all the work to encrypt the transmission is for naught.

• Guard against P2P network applications. If they are allowed to run on your health care network, EHR data will be compromised.

Overall, infrastructure encryption is worth the investment. Though it can never be considered the “silver bullet” for medical record security, it is a best practice for securing EHR data if it’s used appropriately and at multiple hardware levels.
(Continued from page 7)

With data so vulnerable at rest, hardware encryption a must

age the mobile device. The mobile device management (MDM) market is growing as companies realize that these devices have become part of the culture of business and, as a result, are filling with corporate data. Just as IT has had to catch up and encrypt data on laptops, it is going through the same issue with mobile devices.

Many third-party vendors allow encryption on mobile devices. These systems allow for either full-disk encryption, based on the device itself, or encrypted containers where corporate data can be stored and prevented from being brought into the device operating system.

No matter what vendor or encryption scheme is in play, organizations need to be mindful that mobile devices are a large part of the business and that they need to protect the data on these devices with encryption. Without encrypting the corporate data on mobile devices, you put your company at risk.

LEAVE NO UNENCRYPTED PHI IN DATABASES

Our last example focuses on database encryption. While database breaches have been on the rise over the last few years, the practice of database encryption has not grown in step. With the database being the epicenter of all data in a network, it is amazing how many databases still lack proper protection.

If an encrypted database is stolen or breached, and the appropriate tables have been encrypted, the attackers would get nothing useful. To make sure this is the case, all sensitive and confidential data should be encrypted while in the database to protect the records they hold. There should be no protected health information or personal identifiable information left in cleartext in a database for an attacker to siphon out. Review your databases and the data they hold to get a good understanding on what needs to be encrypted.

All in all, encryption is a powerful method to secure the confidentiality of your data—especially data that has the potential to leave your physical premises. Encryption will render data useless to those unauthorized to view it. This increases the protection of your security program and protects the data and records from being compromised. Encryption of data at the hardware level should be an early step in an organization’s defense-in-depth approach. Start early with encryption at this level and it will be easier to keep the data in your organization away from prying eyes. ■
KEEPING UNENCRYPTED PATIENT DATA OUT OF BACKUP TAPES

Backup tapes are a cost-effective option for medical data archiving. Since they contain personal health information, they should be encrypted. Health IT leaders have several options for carrying out this task. BY ALEX ZALTSMAN AND AL GALLANT

MOST HEALTH CARE organizations today use tapes as target media for data backup software. Although disk-to-disk and offsite backup technology has been around for many years, companies continue to use backup tapes as their means for data and disaster recovery. A backup tape can easily expose your organization to a data breach.

Tape backup systems contain at least three components—a tape backup drive, a data backup software application and backup tapes. A typical tape backup configuration is a tape backup drive connected using a cable (usually SCSI or USB) to a server with data backup software installed and configured. The data backup software, such as Symantec Corp. Backup Exec, is programmed to backup data on computers systems on your network. Agents are sometimes deployed to remote systems to enable a faster backup process. Data is backed up over a network, from directly attached (to the backup server) storage devices or storage area networks (SANs). That data is mechanically copied to tape using a proprietary backup format.

If you have electronic personal health information (PHI) on your computer network and it is being backed up to a tape, you should do two things.
First, enable data encryption on the tape backup software. Make sure you understand how data is encrypted and how data is decrypted in case you need to restore it. Make sure the encryption technology is secure (cipher strength, algorithm and so on). For example, if the tape backup is using DES encryption, it is not a secure method of securing your data. AES 128 bit is highly recommended.

In addition, encrypt the data before it is copied to tape. This means you need software to encrypt files on your network. Encrypted data copied over to a tape is secure.

Tapes are susceptible to loss and require people and/or various third parties to store them off site for disaster recovery purposes. Consider moving to an offsite backup service or implement a secure disk-to-disk backup system.

EVALUATE BACKUP TECHNOLOGY CAREFULLY
There are a variety of tape backup technology options, each with their own pros and cons.

- There’s host-based encryption, which works best when encryption is required only for a limited set of data, or even a single stream. As one can imagine, this becomes unwieldy as it scales up.
- There’s in-band appliance encryption, which sits in the middle of a storage connection and encrypts data as it goes from one or more applications to one or more hosts. With so many data paths, this type of encryption can be difficult to engineer.
- Finally, there’s media-based encryption, which encrypts data in media-specific formats. This is the preferred methodology for encrypting tape media, though it should be pointed out that it will have an adverse effect on the performance of media servers.

Don’t neglect the operational impact of these technologies. Physical integration of host-based encryption is fairly straightforward, but it does rely on support from backup software. Appliances, on the other hand, will be harder to integrate into storage infrastructure. Technology
notwithstanding, the impact that tape encryption will have on disaster recovery and data and image archiving must also be considered.

**APPROACH TAPE BACKUP ENCRYPTION CAUTIOUSLY**

Health care CIOs must be aware of the risks associated with unencrypted backup media. If tapes are encrypted, anyone who steals them will have useless media—there will be no breach of medical information; and there will be no fines, penalties or restitution requirements.

For backup media encryption, here are a few tips to keep in mind:

- Hardware-encrypted tapes are the best media to use. They do not use CPU cycles to encrypt while they are backing up data, and they can encrypt at hardware speed. Many of the newest hardware-encrypted backup storage offerings on the market also are the fastest to provide backup services.

- Encrypt close to the destination, not the source. Otherwise, data flexibility and efficiency are lost.

- Don’t lose the encryption keys. Otherwise, you can’t retrieve the data.

- Store the keys separately from the tapes. Storing the keys with the tapes is like printing the combination of the office safe on the safe’s front door.

- To that end, evaluate a tape vendor’s key management system at the same time that you consider an investment in a tape system. By and large, key management systems are not interoperable, so key management should be regarded as a standalone system.

- Use the highest level of tape encryption available. It’s worth the money.

Remember: If tapes are not encrypted, then the Health Information Technology for Economic and Clinical Health Act’s data breach compliance requirements kick in. An organization could pay millions in federal fines, on top of the millions that must be spent on breach notification, consumer credit monitoring and other fees.
Use risk analysis to identify data encryption needs. With data so vulnerable at rest, hardware encryption is a must.

Keeping unencrypted patient data out of backup tapes.

Ali Pabrai is CEO and co-founder of the HIPAA Academy.

Matthew Pascucci has more than 10 years of experience in IT and is currently an information security analyst in the financial sector. He holds multiple certifications and is actively involved with InfraGard to help educate others in information security.

Al Gallant is the director of technical services at Dartmouth-Hitchcock Medical Center in Lebanon, N.H.

Alex Zaltsman is CEO of Experior Data Security and Encryption.

Ali Pabrai is CEO and co-founder of the HIPAA Academy.

Matthew Pascucci has more than 10 years of experience in IT and is currently an information security analyst in the financial sector. He holds multiple certifications and is actively involved with InfraGard to help educate others in information security.

Al Gallant is the director of technical services at Dartmouth-Hitchcock Medical Center in Lebanon, N.H.

Alex Zaltsman is CEO of Experior Data Security and Encryption.