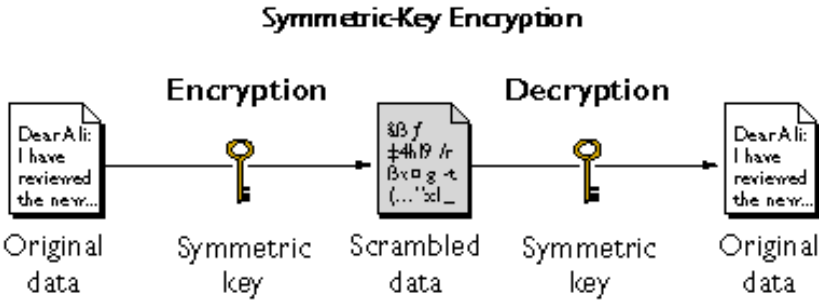
Deciphering the Safe Harbor on Breach Notification:

The Data Encryption Story

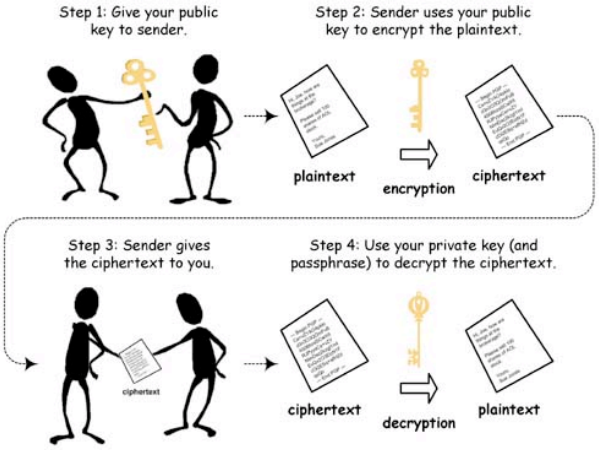
Healthcare organizations planning to protect themselves from breach notification should implement data encryption in their organizations. Data encryption is the only technology recognized by the federal government and many states as a way of making data unusable, unreadable, or indecipherable to unauthorized individuals.

Data encryption is often considered a complex technology that is difficult to implement. However, modern software has made encryption easier to deploy and manage. One of the most important factors that should be used in deciding on an encryption solution is the availability of a centralized management console that can manage the encryption platform. Encryption platforms take into account many points of data protection such as disk encryption, e-mail, file folder, database, etc. Managing encryption software centrally is the key to a successful deployment and management of the encryption solution. The ability to make changes to settings and policies and view log files from a central location is very important.



There are two types encryption methods – symmetric (also called secret key) and public key cryptography (PKI). Symmetric encryption methods are dependant on a passwords or passphrases to encrypt and decrypt data. PKI methods depend on a key pair – a public key and private key to encrypt and decrypt data. Both symmetric and PKI methods could have a place in your encryption deployment strategy.

Care must be taken to ensure that data can be decrypted by management in case an employee leaves, is terminated, or in case of litigation. It is possible to purchase inexpensive off the shelf software to encrypt files or even hard drives. However, without a way for



management to decrypt data you may be putting your organization's critical data at risk of never being recovered. Allowing the use of encryption software that does not have encryption recovery features is strongly discouraged.

So where do you begin? We look at the four areas of concern identified by the government: Data at Rest, Data in Use, Data in Motion, and Data Disposal. Protecting these four areas significantly reduces or eliminates risk exposing unencrypted data to unauthorized individuals.

The government regularly refers to guides published by the National Institute of Standards (NIST). Although these guides were designed to advise federal agencies on securing information they can also be applied to non-governmental entities. After all, data is data regardless of who is storing it. We refer to the appropriate NIST standards documents that pertain to each area of vulnerability.

Data at Rest (NIST SP 800-111): Data at rest is identified as data residing in databases, file systems, flash drives, memory, and structured storage methods. You can simply think of data at rest as data that is stored on various media like internal and external hard drives, USB drives, inside databases, and on file servers. This is stored, but not accessed data. Protecting data at rest can be done using whole disk encryption software. The product you choose should be able to protect data on external devices like USB flash drives, external drives, and network server file shares (note that

accessing file shares could also fall under Data in Motion). Data in databases could also be encrypted (solutions that encrypt individual columns and rows within a table are best used, rather than encrypting the database files themselves).

<u>Data in Motion</u> (NIST SP 800-52, 800-77, and 800-113): Data in motion is identified as data that is moving through the network, including wireless transmission, e-mail, and electronic interchange. Protecting data in motion requires a strategic approach and analysis of existing infrastructure:

- Wireless networks, including Wireless LAN (wifi), Wireless WAN (cellular carrier Internet), and Personal Area Networks (Bluetooth, IrDA). Endpoint policies should be enforced to ensure that data across these connections is encrypted or the technology itself is disabled.

- Wired networks include local area networks and wide area networks. Data should be encrypted at endpoints vulnerable to exposure and each endpoint should have access control technology that can protect the data flowing between these networks.

- E-mails that transfer information with patient information should be encrypted so that only authorized parties can decrypt the information. There are two ways to encrypt e-mail: end to end or at the gateway.

    - End to end e-mail encryption protects e-mails stored inside each e-mail box (either on a server or locally stored on computer). End to end e-mail encryption protects messages from being read by e-mail administrators and anyone that has access to the user's e-mail box or computer (if using POP3 or IMAP to retrieve messages). Although it requires client software to be deployed to all users it is the most

comprehensive method of encrypting e-mail.

  - Gateway encryption does not protect messages in each users mailbox. It does, however, encrypt and decrypt messages as they leave from and arrive to the e-mail server. Gateway encryption is easier to deploy because it does not require client software deployment to each user. Instead, email is encrypted and decrypted using policies or even keywords inside messages. Since all messages are required to pass through an encryption gateway (even emails that do not require encryption) substantial hardware could be required to host the e-mail gateway encryption system. Since the gateway performs the encryption and decryption function the sensitive messages stored in each user's mailbox are decrypted and are not protected.

- Data access between a web portal and web browser should use SSL/TLS. This includes web mail like Microsoft Outlook Web Access and any type of web portal that can contain protected health information.

Data in Use: Data in use is data in the process of being created, retrieved, updated, or deleted. Although there is no specific NIST guide for Data in Use, using a combination of technologies to protect data in use will greatly reduce the risk of unencrypted data being made available to unauthorized individuals. For example, by using whole disk encryption you can be assured that data on a hard drive is encrypted. However, the data is decrypted when it's in use, such as opening a document or a spreadsheet and placing it in memory of the computer. By implementing access control technologies that restrict the type of applications that can run on computers, for example, you can eliminate the threat of malware. Adding smart cards or tokens will eliminate the threat of unauthorized use of the computer. Monitoring your network for data leakage and intrusion will protect the overall data infrastructure.

<u>Data Disposed</u> (NIST 800-88): Data disposed means discarded paper records or recycled electronic media (especially hard drives located in discarded personal and laptop computers). Digital media must be appropriately disposed or properly wiped using industry-standard applications. There are two ways to destroy digital data:

- Software method – Use software that wipes data multiple times from the media. This type of specialized software replaces existing data with random data. Overwriting existing data multiple times, as many as 3 times, is recommended. Note that this method is very time consuming, although the media could be reused after being securely overwritten.

- Hardware method – You can use a degaussing devices to wipe data from media. Degaussing requires special equipment compliant with National Security Agency standard NSA/CSS-EPL-9-12A-B.

- Shredding – Media could be shredded by using special shredding equipment that is similar to paper shredders. Hard drives and flash drives are literally shred in to scrap metal.

After implementing your data security and encryption technologies it's important to regularly review and audit these systems. Below are some suggested points for auditing your information systems:

- Indentify a person or group of people responsible for oversight of your encryption and data security strategy.

- Physical & Environmental Security
    - Implement physical security controls around your data equipment. This could include placing computer equipment in locked rooms that only authorized individuals could access. Servers and networking equipment could be further secured by placing them into locked cabinets.

- Implement computerized card access or similar systems instead of metal keys so that access logs could be maintained and privileges to room access could be easily revoked.

- Do not leave computer and networking equipment in unsecured areas

- Formal policies prohibiting the use of unauthorized software.

- Review firewall access lists and maintain a change log to firewall configurations.

- Review content filtering systems to ensure they are functioning properly.

- Implement a network intrusion protection system where appropriate.

- Formal policy on data disposal including written procedures for disposing of computer equipment and media.

- Existence and proper operation of endpoint control and malicious software detection software.

- Maintain separation duties between system administrators and administrators of encryption technologies whenever possible or appropriate.

- Network access control - users should be provided with access to only network resources they need to perform their task.

- Remote access systems should have appropriate encryption activated and proper user authentication systems in place. If possible, implement and test two-factor authentication systems.

- Individual user accounts with strong password requirements are issued to employees who need access to computing and network resources.

- Telecommuting access should be provided on equipment owned and controlled by your organization and should have endpoint security software installed and tested.

- Documented company encryption and access control policies that maintain your organizations policy on data encryption, recovery of encrypted data, control of smart cards/access tokens, and key management policies. Company employees should also be trained on what types of data should be encrypted.

Reviewing your policies and controls should be done quarterly and logs should be maintained.

Deployment Methods

There are two ways to implement data encryption:

- On-Premise: Implementing your own data encryption solution requires you to purchase and maintain hardware and software to host the management console for the data encryption platform. Staff will need to be trained on how to deploy and maintain the solution. Customers need to ensure that the management server is backed up. Some encryption solutions use a SQL server backend, which requires its own database maintenance and backup.

- On-Demand: A managed service provider could host the management console. Client software would be deployed to all endpoint devices. Policies could be deployed and managed centrally. This solution does not require you to purchase and maintain your own hardware and software. Training for staff is limited to client deployment and learning about the settings of the client application.

As an example, Experior deploys encryption using both methods, depending on customer preference. However, On-Demand (or "cloud") is becoming more preferred because there is no investment in hardware, software, and licensing for the customer. The solution can be rolled out quickly without the need for the customer purchase and configure servers.

Purchasing the appropriate solution is only half of the equation. In addition to choosing the proper technology your organization needs to choose a vendor with experience in implementing and maintaining data security technologies.

About Experior Data Security and Encryption

Experior Data Security and Encryption is a managed service provider and professional services firm specializing in helping customers comply with federal regulations related to health care such as the American Recovery and Reinvestment Act of 2009 (ARRA) and the Healthcare Insurance Portability and Accountability Act (HIPAA). Experior Data differentiates itself by specializing in security and encryption of health records to ensure that health care organizations meet and/or exceed government requirements for securing protected health information.

Experior Data Security and Encryption Data is a Silver Partner with PGP Corporation, a global leader in email and data encryption software for Enterprise Data Protection. PGP's software is used by more than 110,000 enterprises, businesses, and governments worldwide, including 96 percent of the Fortune® 100, 74 percent of Fortune® Global 100, 80 percent of the German DAX Index and 71 percent of the United Kingdom FTSE 100 Index.

Article written by Alex Zaltsman, CEO of Experior Data Security & Encryption. Experior specializes in implementing and maintaining data encryption and security solutions. Experior Data's web site is www.experiordata.com Follow their twitter feed at @experiordata.