HIPAA Security Rule: Frequently asked questions regarding encryption of personal health information

Please note that some of the links below may take you off the AMA Web site. The AMA is not responsible for the content of other Web sites.

The Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act of 2009, has made several important changes to the HIPAA Security Rule. These changes have raised a number of questions among physicians and other health care professionals as well as other HIPAA-covered entities and business associates.[*] This resource addresses the most common of these questions.

1. I manage a small practice. Why should I care about the changes to the HIPAA Security Rule?

Perhaps the most significant of the changes to the HIPAA Security Rule is the requirement for HIPAA-covered entities and their business associates to provide notification in the event of a breach of "unsecured protected health information [PHI]." This means, for example, that if a hacker were able to gain access to a physician practice's computer system that contained patient information, the physician practice would have to inform all patients and the Department of Health and Human Services (HHS) of the breach. In some cases, the physician practice would also need to notify the media.

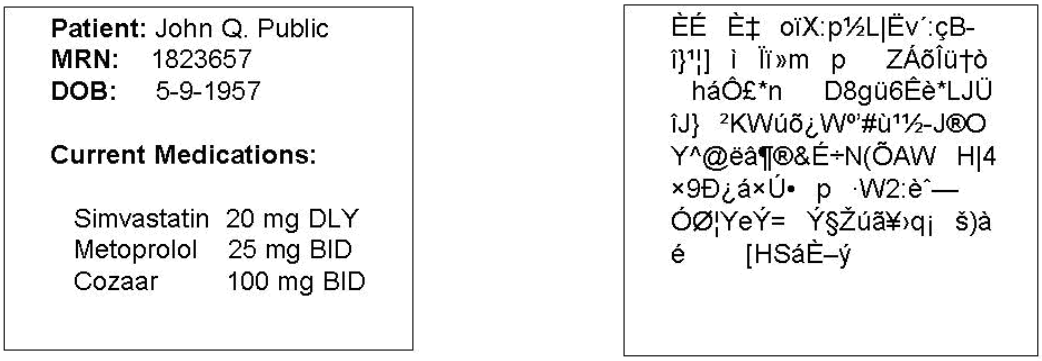
The one and only exception to this new requirement is encryption technology: **If the electronic PHI (or *e*PHI) is stored and transmitted in encrypted form, then you do not need to notify patients, even if there is a security breach.** The National Institute of Standards and Technology (NIST) has issued Special Publication 800–66–Revision 1, "**An Introductory Resource Guide for Implementing the HIPAA Security Rule**," which is intended to describe the technologies and methodologies that physicians and other HIPAA-covered entities and their business associates can use to render *e*PHI unusable, unreadable or indecipherable to unauthorized individuals. While HIPAA-covered entities and their business associates are not required to follow this guidance, if your practice does follow the specified technologies and methodologies, you will avoid having to comply with the extensive notification requirements otherwise required by the HITECH Act in the event of a security breach.

[*] Visit **www.cms.hhs.gov/HIPAAGenInfo/06_AreYouaCoveredEntity.asp** to learn more about who is considered a HIPAA-covered entity.

2. What is encryption exactly?

Encryption is a technique for transforming information in such a way that it becomes unreadable. This means that even if a hacker is able to gain access to a computer that contains PHI, he or she will not be able to read or interpret that information. The patient's privacy will still be protected.

Figure 1: Encrypted data



Unencrypted data ("plaintext")

Encrypted data ("ciphertext")

3. How does encryption work?

Encryption is done either by computer programs or by specially designed computer hardware devices. These programs or devices apply a mathematical algorithm (i.e., a recipe for producing encrypted data) to the information. The output is a scrambled form of the original data. When a legitimate user needs to access the data, the scrambling process is reversed, and the data is restored to its original form. Only those who are in possession of the "key" can unscramble (i.e., "decrypt") the data.

4. What is a "key?"

A key is a piece of data that an encryption algorithm uses to determine exactly how to unscramble the protected information. It is called a key because it "unlocks" the encryption formula to unscramble the encrypted data.

5. I keep seeing abbreviations such as "RSA" and "AES." What do these abbreviations mean?

These abbreviations are the names of specific mathematical algorithms. Algorithms are like recipes. Algorithms specify the ingredients (the key and the "plaintext" data to be protected) and the specific steps that need to be taken to produce the output (the "ciphertext," or encrypted data) from the information that is inputted. "RSA" gets its name from its inventors—Ron Rivest, Idi Shamir and Leonard Adelman—and "AES" stands for "advanced encryption standard." Other encryption algorithm names include "DES," "Triple-DES" (or "3DES"), "Rijndael," "Twofish," "MARS" and "Serpent."

6. People talk about "public" and "private" keys. What is the difference?

Actually, there are three types of keys: "secret," "public" and "private." Different encryption algorithms use different types of keys. The more traditional encryption schemes use secret keys to both encrypt and decrypt data. Newer methods of encryption, known as "public-key" algorithms, use a public key to encrypt a piece of information and its corresponding private key to decrypt the information. (This kind of encryption is like a post office box. Anyone can put a letter in the box, but only the owner of the box can take the letter out.)

Figure 2: Types of keys

Secret-key cryptography

Bob and Alice share a secret key. Bob and Alice encrypt the data using the same key.

Public-key cryptography

Alice has “public” and “private” keys. Bob encrypts the data using Alice’s public key. Only Alice can decrypt the data because only she has the private key.

7. Which types of data can be encrypted?

Any kind of data can be encrypted. You can encrypt plaintext files, PDF documents, spreadsheets, images and any other form of information in your computer. You can even encrypt database information and information on back-up media.

8. Which data should a physician practice typically encrypt?

You should encrypt any systems and individual files containing *e*PHI. Data you should encrypt includes your practice management system; electronic medical records; documents containing *e*PHI, such as claims payment appeals; scanned images, such as copies of remittance advices; e-mails containing *e*PHI; and *e*PHI that you transmit, such as the claims sent to a clearinghouse.

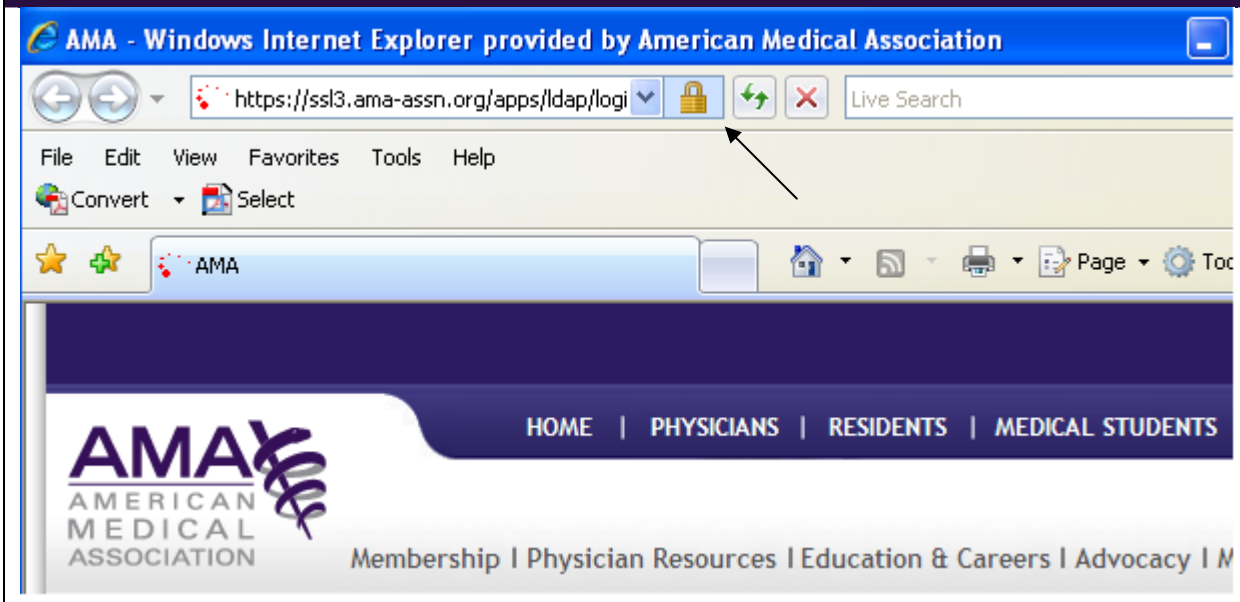
9. Do e-mails containing *e*PHI have to be encrypted?

Yes, e-mails containing *e*PHI must be encrypted. E-mail is not like mailing a sealed letter or package. It is more like sending a postcard. People are not supposed to read it while it is in transit, but it passes through many hands, and one can never be sure that someone is not reading it illegally. Fortunately, there are many tools available for encrypting e-mail.

10. Does *e*PHI that is accessed via the Internet need to be encrypted?

Yes, data that is published on the Internet is available to the public. The only way to protect health information that is made available on a Web site is to use a technology known as “secure sockets layer” (SSL). You are probably already using this encryption method, whether you are aware of it or not. Any Web site that has a URL (i.e., an Internet address) beginning with “https” is using SSL or a similar encryption method. When you are on these Web sites, you may notice a small padlock icon on your browser. Double-clicking this icon usually gives you more information about how that browsing session is protected.

Figure 3: SSL protection



11. Is it difficult to encrypt data?

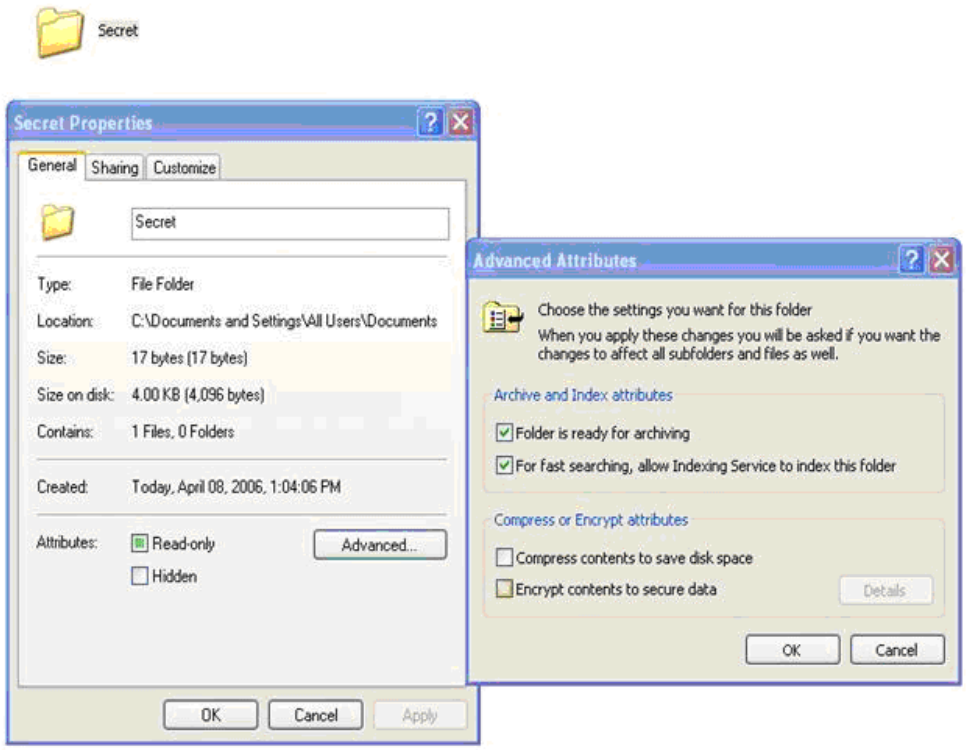
The difficulties involved in encrypting sensitive information depend on the method you choose. There are many possible approaches to implementing data encryption practices. Typically, a system administrator will make an initial investment of time and effort to install and configure the encryption products. Physician practices that do not employ a full-time system administrator may need to work with a contractor to accomplish the necessary set-up tasks. In many cases, you will need to work with your electronic medical transcription or practice management system vendor to have them implement the appropriate encryption technology on your system and to configure it properly.

After initial implementation, the process of encrypting and decrypting data should be virtually automatic—the most user involvement encryption may require is minimal effort to specify which data items should be encrypted. If the installation and set-up are completed properly, you should not experience any impact at all on workflow or normal operations.

12. How can I encrypt the data on my computers?

You have several choices. There are built-in encryption programs, such as Microsoft® Encrypting File System (EFS), which you can use simply by changing the properties of the folder in which the sensitive data is kept (if you use a computer with Microsoft Windows®). Most of the popular database technologies, such as Microsoft SQLServer®, MySQL®, Oracle® and Sybase®, include an encryption option you can use. There are also several encryption products, such as Pretty Good Privacy® (PGP®), that you can purchase and install on your computer.

Figure 4: Sample encryption program



Microsoft Encrypting File System is one example of easy-to-use encrypting software.

13. Is encryption expensive?

Encryption can be expensive, but it doesn't have to be. Some encryption programs are available at no cost. Microsoft EFS, for example, is shipped as part of the Windows operating system. Microsoft also provides whole-disk encryption on Windows 7 systems with a program called BitLocker™ Drive Encryption. Other programs, such as TrueCrypt®, may be downloaded and installed for free. At the other extreme, encryption devices known as hardware security modules (HSMs) can be quite expensive. The choice you make depends on many factors, including encryption strength, speed, available technical support and ease of use.

14. What is the best encryption technology to use?

In 2000, NIST sponsored a competition to identify the best available encryption algorithm. The Rijndael algorithm won the competition hands down. This algorithm has been designated as the current advanced encryption standard (AES). AES is a good choice for protecting *e*PHI.

The most widely used public-key algorithm is RSA. But this algorithm is not a good choice for protecting *e*PHI because it is much slower than AES. However, RSA is an excellent choice for encrypting electronic signatures and exchanging keys. A newer public-key algorithm is known as "elliptic curve cryptography" (ECC). NIST has specified a preference for ECC over RSA in future government procurement because ECC is believed to be stronger and faster than RSA.

The HHS Office for Civil Rights (OCR) has published guidance on choosing an encryption method on its **Web site**. The OCR guidance identifies ways to avoid the breach notification requirement—including recommended

processes by NIST—and provides information on the new HIPAA breach notification requirements that HIPAA-covered entities must comply with. Following are several NIST publications that you may find useful:

- NIST Special Publication 800-111, "**Guide to Storage Encryption Technologies for End-User Devices**," provides extensive information on encrypting data on laptops
- NIST Special Publication 800-52, "**Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations**," includes detailed information on technologies that are used to protect sensitive Web site information
- NIST Special Publications 800-77, "**Guide to IPsec VPNs**," and 800-113, "**Guide to SSL VPNs**," provide guidance on selecting the appropriate technology for establishing virtual private networks

Visit **www.csrc.nist.gov/publications/PubsSPs.html** to download all NIST Special Publications titles free of charge.

The OCR guidance also references the Federal Information Processing Standard (FIPS) 140-2, "**Security Requirements for Cryptographic Modules**." This standard describes a rating system that is used to evaluate commercial encryption products and assign a security level to them. Visit **www.csrc.nist.gov/publications/PubsFIPS.html** to download all FIPS publications free of charge.

15. Where are the keys kept?

Keys can be stored in a number of different places. Sometimes keys are kept on smart cards, USB flash drives or similar devices. Sometimes keys are stored on "key server" devices in a computer network. Sometimes keys are not stored anywhere at all but are regenerated when they are needed. Sometimes keys are stored on the same computers that contain the encrypted data—but this is considered to be a very insecure arrangement. HHS notes that an entity is **not** exempt from the breach notification requirements if the entity keeps the keys on the same device as the encrypted data.

For this reason, it is important that you know where your keys are kept. If the location of the key storage is not made clear in the product documentation, then you should ask your vendor before selecting a product for your practice. A number of encryption products allow you to choose where the keys are kept as an option during installation or configuration. Microsoft EFS, for example, allows you to decide whether the keys are kept on the same system as the encrypted data, on a floppy disk that you can remove from the system and store separately, or not stored at all but rather regenerated from a user-supplied password when needed.

Some people find it helpful to keep their key on an encrypted USB flash drive that they keep on their key chain with their car keys. To unencrypt their data, they just insert the flash drive and type in their password. For added security, it is even possible to get a flash drive with a thumb-print reader that is programmed to recognize only the user's thumb print.

16. What if a hacker finds the key?

If a hacker finds the key, the encrypted data to which that key provides access is no longer safe. That is why it is never a good idea to keep the key on the same device as the encrypted data. Visit **www.ama-assn.org/go/pmc** to access "**Steps physicians should take if in danger of identity theft**" for more information about protecting data that is no longer safe.

17. Why are people concerned about key size?

Key size can indicate how weak or strong the encryption is. As a general rule, the greater the key size, the better the data is protected (e.g., a 256-bit key generally provides better protection than a 128-bit key). However, this is not always true. For example, data encrypted with the RSA algorithm using a 256-bit key is not as safe as data encrypted using the AES algorithm using a 128-bit key.

Most encryption products allow you to choose which encryption algorithm and which key size you will use. You are usually given a chance to make these decisions as an option during installation or configuration. While a larger key size generally provides greater protection, it can also result in slower performance. You will need to decide whether the slower performance is an acceptable trade-off for the greater security.

18. Can anything else go wrong?

One possible problem would be losing the encryption key and not being able to retrieve the encrypted information when you need it. **Make sure you have a back up of the key in a safe place.** Another problem would be using an old encryption algorithm, such as the "data encryption standard" (DES), that is no longer considered secure. Hackers have figured out how to break these out-of-date encryption standards and have even published their findings on the Internet. Yet another problem is not sufficiently protecting encryption keys. Using the strongest possible encryption method does not protect patient information if a hacker can find a way to break the security used to protect the keys.

19. I'm convinced that I need to encrypt my sensitive data. What should I do?

First, you need to tend to the most pressing problem areas. Refer to NIST Special Publication 800–66–Revision 1, "**An Introductory Resource Guide for Implementing the HIPAA Security Rule**," for guidance in addressing these areas.

- Encrypt any back-up media that leave your building.

  If you send back-up media to a vault, disaster recovery site or any other location, then any one of these items going astray would trigger a breach notification situation. This means that the back-up program that you use must include an encryption step. Fortunately, there are many back-up products that include this capability. Perform an Internet search on "back-up encryption software" to obtain a list of products that might fit your needs.

- Encrypt any e-mail that contains *e*PHI.

  If you currently correspond with patients, health insurers or other health care professionals via e-mail and those e-mails contain *e*PHI, then you could be accused of failing to protect *e*PHI for which you are responsible. There are two basic approaches to encrypting e-mail: PGP and S/MIME. PGP is a technology that was pioneered by the PGP Corporation, and S/MIME is the e-mail encryption capability that is built into Microsoft Outlook®. But these two are not the only e-mail encryption product vendors. Perform an Internet search on "e-mail encryption software" to get a more complete list of your options.

- Encrypt any laptops that contain *e*PHI.

  Even laptops that are protected with strong "boot passwords" are vulnerable. This is because a hacker can remove the hard drive from a stolen laptop and install it in a system that he or she controls. Only encryption can protect PHI on a laptop. Microsoft EFS, which is installed by default on all Windows systems, offers some protection, but "whole disk encryption" technology is a more secure solution. Perform an Internet search on "whole disk encryption software" to get an idea of products to consider.

- If *e*PHI is accessed via the Internet, encrypt these sessions.

  Check with your Web designer or Web services provider to ensure that any PHI that travels across the Internet is protected by SSL, TLS or similar technology.

- Encrypt any other remote access sessions.

  If you have situations in which physicians or staff from your practice connect to the home office remotely, such as physicians attending conferences who connect to read e-mail or access other resources containing *e*PHI, then this access may constitute a vulnerability to unauthorized snooping. It is important that these sessions be conducted using encrypted "tunnels," known as "virtual private networks" (VPNs). You have

many options for implementing VPNs in your environment. Perform an Internet search on "virtual private networks" for more information. (Note that VPN technology usually requires experienced professional help to install and configure.)

Once you have addressed these areas, you can then consider the pros and cons of encrypting "data at rest" (data that never leaves your facility, such as data kept in your practice management system or other electronic medical record databases). Some people choose to encrypt all *e*PHI so that they have a "safety net" in the event that a hacker manages to penetrate their network defenses. Other people encrypt only that portion of the *e*PHI that actually leaves their facility. You should consider the recommendations of the OCR guidance as well as the cost/benefit tradeoffs before making a decision for your practice.

20. Where can I learn more?

The quickest and easiest way to obtain some good information is to perform an Internet search on "HIPAA PHI encryption." Many companies that sell HIPAA compliance solutions offer training and consulting advice in this area. Vendors who provide encryption hardware and software provide information in the form of "white papers" that are available through their Web sites. Technical support services, such as Microsoft TechNet, provide detailed information on configuring and using specific encryption products.

Following is a brief list of online resources if you wish to explore this subject further:

- RSA Laboratories Cryptography frequently asked questions (**www.rsasecurity.com/rsalabs/node.asp?id=2152**)
- The PKI Pages (**www.pki-page.org/**)
- History of Cryptography (**http://world.std.com/~cme/html/timeline.html**)
- List of Encryption Products (**www.timberlinetechnologies.com/products/encryption.html**)

Visit the HHS Web site at **www.hhs.gov/ocr/privacy/** for updated guidance on encryption technology.

Questions or concerns about practice management issues?

AMA members and their practice staff may e-mail the AMA Practice Management Center at **practicemanagementcenter@ama-assn.org** for assistance.

For additional information and resources, there are three easy ways to contact the AMA Practice Management Center:

- Call **(800) 621-8335** and ask for the AMA Practice Management Center.
- Fax information to **(312) 464-5541**.
- Visit **www.ama-assn.org/go/pmc** to access the AMA Practice Management Center Web site.

Physicians and their practice staff can also visit **www.ama-assn.org/go/pmalerts** to sign up for free Practice Management Alerts, which help you stay up to date on unfair payer practices, ways to counter these practices, and practice management resources and tools.

The Practice Management Center is a resource of the AMA Private Sector Advocacy unit.