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

The Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act of 2009, made several important changes to the HIPAA Security Rule. These changes have raised a number of questions about encryption among physicians and other health care professionals as well as other HIPAA-covered entities and business associates.[1] This resource addresses the most common of these questions. Physicians should also note that states may have laws and regulations that go above and beyond the federal requirements outlined in this fact sheet and should confirm if any local requirements may apply.

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

Perhaps the most significant change 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 (unsecured PHI)." For more information on breaches of unsecured information see our Breach Notification Fact Sheet. This means, for example, that if a hacker were able to gain access to a physician practice's computer system, laptop, tablet, PDA, etc. that contained PHI that was not encrypted, the physician practice may need to notify the affected 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. Therefore, not only can lack of compliance result in reputational harm to your practice, it can risk exposure of your patient's most sensitive information.

2. How can I mitigate the HIPAA breach notification requirements?

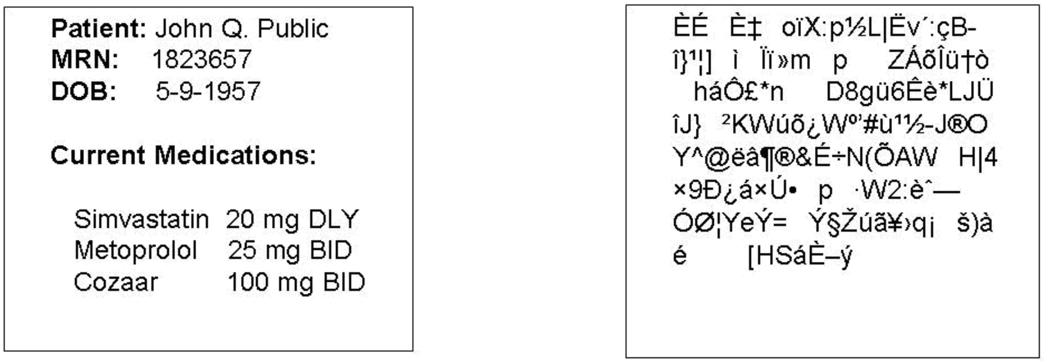
By storing and transmitting your data in an encrypted form. **If the electronic PHI (or ePHI) is stored and transmitted in encrypted form, then you do not need to notify patients, even if there is a security breach.** The National Institute of Standards and Technology (NIST), an institute within the Department of Commerce that establishes standards for a variety of industries including health care, has issued Special Publication 800–66–Revision 1, "An Introductory Resource Guide for Implementing the HIPAA Security Rule," that describes the technologies and methodologies that physicians and other HIPAA-covered entities and their business associates can use to render ePHI unusable, unreadable or indecipherable to unauthorized individuals. This is extremely technical guidance, and the AMA recommends physicians work with their software vendors to ensure their computers and electronic devices have acceptable encryption software loaded. The HIPAA Omnibus Rule published January 25, 2013, reaffirmed that encryption and destruction, consistent with NIST guidelines, would alleviate notification in the event of a breach. While HIPAA-covered entities and their business associates are not required to follow this guidance, if your practice does implement 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.

[1] Visit https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/Downloads/CoveredEntitiesChart20160617.pdf to learn more about who is considered a HIPAA-covered entity.

3. What is encryption exactly?

Very simply, you can think of encryption as a locked door with your patient's PHI on the inside of the door and the only way to access it is if you have the key. The way encryption works is by transforming information so 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



Patient: John Q. Public
MRN: 1823657
DOB: 5-9-1957

Current Medications:

Simvastatin	20 mg DLY
Metoprolol	25 mg BID
Cozaar	100 mg BID

Unencrypted data ("plaintext")

```
ÈÉ  È‡  oïX:p½L|Ëv´:çB-
î}¹¦]  ì  Ïï»m  p    ZÁõÎü†ò
  háÔ£*n    D8gü6Êè*LJÜ
îJ}  ²KWúõ¿Wº'#ù¹½-J®O
Y^@ëâ¶®&É÷N(ÕAW  H|4
×9Ð¿á×Ú•  p  ·W2:èˆ—
ÓØ¦YeÝ=  Ý§Žúã¥›q¡  š)à
é      [HSáÈ–ý
```

Encrypted data ("ciphertext")

4. 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.

5. 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.

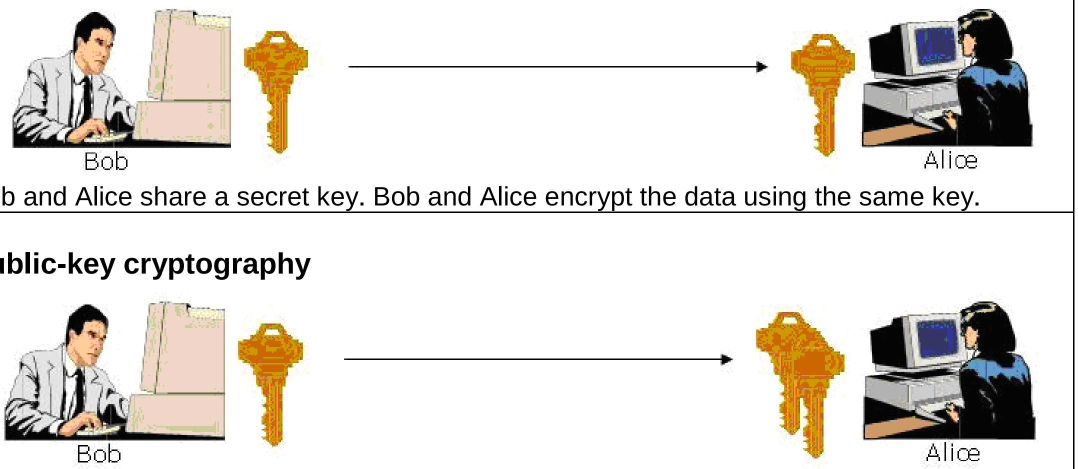
6. I keep seeing abbreviations such as "RSA" and "AES." What do these abbreviations mean?

These abbreviations are the names of specific mathematical algorithms. Algorithms are like recipes in that they 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, Adi 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."

7. People talk about “secret,” “public” and “private” keys. What is the difference?

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.

8. Which types of data can be encrypted?

Encryption can be used to protect data at rest, such as files on computers and storage devices, and data in transit; for example, data being transferred via the Internet. 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.

9. Which data should a physician practice typically encrypt?

You should encrypt any electronic systems and individual files containing PHI that is stored electronically, otherwise known as ePHI. Data you should encrypt includes your practice management system; electronic medical records; claims payment appeals; scanned images, such as copies of remittance advices; emails containing ePHI; ePHI that you transmit, such as the claims sent to a clearinghouse; and any back-ups you make of your electronic systems or files.

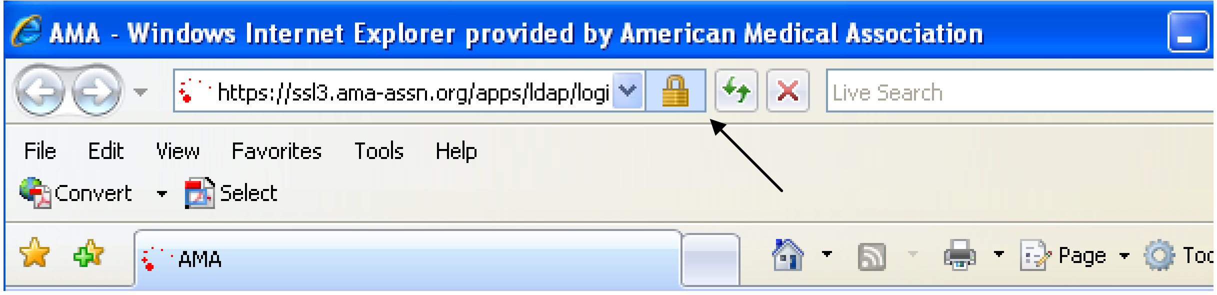
10. Do emails containing ePHI have to be encrypted?

Although law permits physicians to send PHI through unsecure email, it is not recommended as the information could be breached by an unauthorized party. Therefore, the AMA recommends physicians use encrypted email when sending ePHI. Email is not like mailing a sealed letter or package. It is more like sending a postcard – people are not supposed to read it while 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 email. However, if a physician wants to use unsecure email to communicate with patients, they should consider seeking the patient's written permission and explain the risks of doing so.

11. Does ePHI that is accessed via the Internet need to be encrypted?

Yes. Since ePHI that is published on the Internet is available to the public it needs to be encrypted otherwise anyone can view it. To make PHI available on a web site requires a technology known as "secure sockets layer/transport layer security" (SSL/TLS). You are probably already using this encryption method, whether you are aware of it or not. Most major online retailers, for instance, use this to protect your information when you make an online purchase. Web sites and their associated web servers make use of SSL/TLS in conjunction with traditional hypertext transfer protocol (HTTP) to establish a secure connection. Any web site that has a URL (i.e., an Internet address) beginning with "https" is using SSL/TLS or a similar encryption method. This process provides a reasonable guarantee that the communication between website and web browser is secure and cannot be viewed by a third party. 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


AMA - Windows Internet Explorer provided by American Medical Association
https://ssl3.ama-assn.org/apps/ldap/logi
Live Search
File
Edit
View
Favorites
Tools
Help
Convert
Select
AMA
Page
Too

12. Is it difficult to encrypt data?

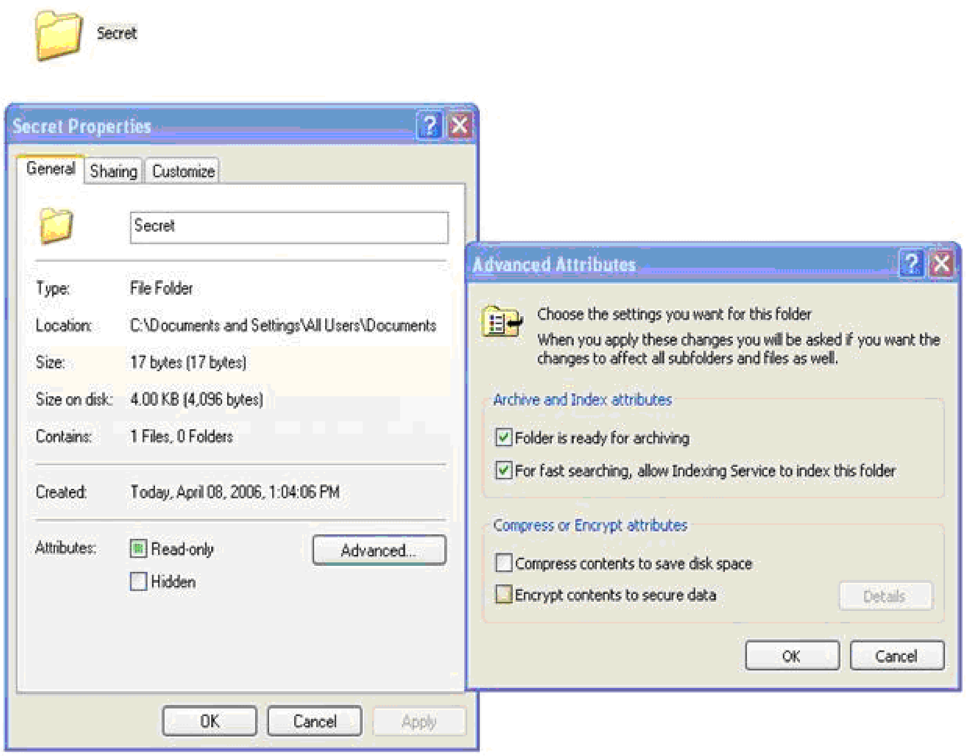
The difficulties involved in encrypting sensitive information depend on the method you choose. Typically, a system administrator will make an initial investment to configure the encryption products. Physician practices that do not employ a full-time system administrator may need to work with a contractor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

After initial implementation, the process of encrypting and decrypting data should be virtually automatic; user involvement is typically minimal, requiring entities to specify which data items should be encrypted. If the installation and set-up are completed properly, you should not experience any impact on workflow or normal operations.

13. 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. BitLocker Drive Encryption is an additional security feature that is also included with the Microsoft Windows® operating system. If you use an operating system other than Microsoft Windows®, there may be encryption functionality that is distributed as a standard feature of that architecture. Mac OS X®, from Apple Inc., for example, includes the File Vault 2 program, which is similar in functionality to BitLocker. There are file and full disk encryption options that are freely available for the various flavors of Linux distributions as well. 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



Secret

Type: File Folder

Location: C:\Documents and Settings\All Users\Documents

Size: 17 bytes (17 bytes)

Size on disk: 4.00 KB (4,096 bytes)

Contains: 1 Files, 0 Folders

Created: Today, April 08, 2006, 1:04:06 PM

Attributes: ☑ Read-only ☐ Hidden

Choose the settings you want for this folder

When you apply these changes you will be asked if you want the changes to affect all subfolders and files as well.

Archive and Index attributes

☑ Folder is ready for archiving

☑ For fast searching, allow Indexing Service to index this folder

Compress or Encrypt attributes

☐ Compress contents to save disk space

☐ Encrypt contents to secure data

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

14. Is encryption expensive?

Encryption can be expensive, but it doesn’t have to be.

As noted in the previous question, most major operating system vendors include cryptographic utility programs in the software that is distributed with their operating systems. Other programs, such as TrueCrypt®, may be downloaded and installed for free. Many practices have been able to satisfy all or most of their ePHI encryption needs through the use of the SSL/TLS technology that is built into essentially all web servers and browsers. Practice web sites can be configured to provide confidential communication with patients and to allow remote access (such as physicians attending conferences) to ePHI.

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.

15. What is considered among the best encryption technology?

In 2000, NIST sponsored a competition to identify the best available secret key encryption algorithm. The Rijndael algorithm won the competition and has been designated as the current Advanced Encryption Standard (AES).

The most widely used public-key algorithm is RSA; however, this algorithm is slower than AES and may be difficult to use for ePHI. RSA, however, is an excellent choice for encrypting electronic signatures and exchanging keys. A newer public-key algorithm is "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 website.

The following are several NIST publications that are referenced in this guidance and may provide additional information:

- NIST Special Publication 800-111, "Guide to Storage Encryption Technologies for End-User Devices," provides extensive information on encrypting data on laptops
- 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

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 assigns a security level to them. NIST evaluates commercial encryption products and ensures that they adhere to proper cryptographic security standards. The Cryptographic Module Validation Program (CMVP) tests hardware products and the Cryptographic Algorithm Validation Program (CAVP) tests software products. View a list of CMVP-validated products, and a list of CAVP-validated products. (All FIPS publications are also available for download free of charge.)

16. Where are the "keys" kept?

Keys used to encrypt and decrypt PHI can be stored in a number of different places. Keys can be 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 in the form of a one-time number when they are needed. Keys can also be stored on the same computers that contain the encrypted data—but this is considered to be a very insecure arrangement, and is not recommended. **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 CD-ROM that you can remove from the system and store separately, or not stored at all but rather regenerated in the form of a one-time number when a user-supplied password is used.

Some people keep keys and other security information on encrypted USB flash drives. This allows individuals to keep the keys physically with them at all times (on a key ring, for example) and not on the system that contains the encrypted ePHI. The data can be accessed when needed by inserting it into a computer USB port and entering a password when prompted. For added security, one can obtain a flash drive that is equipped with a thumb print reader. The SanDisk Cruzer® Profile Biometric USB Flash Drive is one example of this technology. Perform an Internet search on “fingerprint flash drives” to get a more complete vendor list.

17. 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.

18. 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 protection (e.g., a 256-bit key generally provides better protection than a 128-bit key), though this may not always be the case.

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.

19. Can anything else go wrong?

One possible problem is losing the encryption key and not being able to retrieve the encrypted information when you need it. **Make sure you have back-up copies of all encryption keys in a safe place.** Another problem can arise from 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 failing to protect encryption keys. Using the strongest possible encryption method does not protect PHI if a hacker can find a way to break the security used to protect the keys.

20. 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 leaves your building.
  If you send back-up media to a vault, disaster recovery site or any other location, the PHI stored should be encrypted otherwise a breach of unencrypted information will trigger breach notification requirements. Therefore, the back-up program you use should 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. (Don’t forget to send copies of the encryption keys to the disaster recovery site – but remember not to put them on the same truck as the backup tapes themselves.)
- Encrypt any email that contains ePHI.
  If you currently correspond with patients, health insurers or other health care professionals via email and those emails contain ePHI, then you could be susceptible to a security breach. There are two basic approaches to encrypting email: PGP and S/MIME. PGP is a technology that was pioneered by the PGP Corporation, and S/MIME is the email encryption capability that is built

into Microsoft Outlook®. For other options, perform an Internet search on “email encryption software.”

- Encrypt any laptops that contain ePHI.
  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 ePHI is accessed via the Internet, encrypt these sessions.
  Some practices provide interactive web environments like patient portals from which patients may interact remotely with doctors, nurses and staff. Such systems allow patients to send and receive messages, schedule appointments, review test results and request prescription refills from the convenience of their homes. Some web-enabled products such as MyChart from Epic Systems Corporation incorporate cryptographic protection of ePHI automatically. There are several other vendors who offer similar built-in protection. Perform an Internet search on “online health information software” to get a more complete list of your options.
- Encrypt any other remote access sessions.
  There are situations in which personnel need to access your information systems from a remote location. If, for example, physicians who are attending a conference connect to read email or to access other resources containing ePHI, 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). Most companies, for instance, require the use of a VPN for remote access to their networks by employees, especially when using home computers. 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 office). Increasingly, with the movement to health information exchanges and patient portals, more and more data is expected to move outside the walls of your office. Some people choose to encrypt all ePHI 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 ePHI that actually leaves their office. You should consider the OCR’s guidance as well as the cost/benefit tradeoffs before making a decision for your practice.

21. Where can I learn more?

Many companies that sell HIPAA compliance solutions offer training and consulting advice. 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.

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

- HHS website on mobile device privacy and security
- HHS Security Guidance on Mobile Devices
- Lists of Encryption Products:
  - CMVP
  - CAVP

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