Laptop Encryption Project Update

- All university laptops are being encrypted to ensure that if the device is lost or stolen the contents cannot be accessed by unauthorized individuals – this is faster and cheaper than constant data inventories and risk of having to perform disclosures
- Approximately 515 laptops encrypted out of 2000
- Project deadlines now set for departmental IT staff:
  - September 1\textsuperscript{st}: Attend training and schedule laptops for encryption
  - December 31\textsuperscript{st}: Complete encryption project
- Stimulus legislation rules requiring increased protection for patient health information expected in September:
  - Non-encrypted devices containing patient information that are lost will require mandatory media & patient notification
  - Individuals losing patient information can be subject to increased fines and civil penalties
- Need your help to ensure the encryption project is a high priority for departmental IT staff
- Requests for additional time will be evaluated for risk of data loss – no more than 2-3 month extensions are expected to be offered
Why Encryption?

Buried deep within the 1,000-plus pages of the American Recovery and Reinvestment Act of 2009 (ARRA) are sweeping changes to the health information privacy and security regulations of the Health Insurance Portability and Accountability Act (HIPAA). Previously, covered entities were obligated to mitigate harm caused by unauthorized disclosures of Protected Health Information (PHI), but not required to give notice to the individuals whose information was inappropriately disclosed. Going forward, covered entities and business associates will be required to notify individuals when security breaches occur with respect to "unsecured" information. Unsecured information means information not protected through technology or methods designated by the federal government. Preliminary guidance suggests interpretation of the term “unsecured” will include unencrypted email messages containing PHI. The loss of portable media devices housing PHI will also be considered breaches if the devices are not secured with encryption protections. Notification must occur within 60 days of discovery of the breach and a report of all breaches must be submitted to the federal Department of Health and Human Services annually. Additionally, if the breach involves 500 or more individuals, public media notification is also required.

ARRA gives power to state attorney generals to bring actions to obtain injunctive relief or damages on behalf of state residents who have been, or are threatened or adversely affected by violations of HIPAA. Previously, HIPAA did not permit individuals to obtain monetary damages for HIPAA violations and enforcement was handled at the federal level.

Civil Penalties and Enforcement: The new law expands the existing civil penalty provisions, which are effective for all violations after the date of enactment of ARRA (February 17, 2009). The civil penalties have increased substantially and are categorized by type as follows:

- **Tier 1** – Where the person is unaware of the violation, and would not have known even with reasonable diligence, the penalty is at least $100 per violation not to exceed $25,000 for all violations of the same requirement during the year.
- **Tier 2** – Where the violation is due to "reasonable cause" and not willful neglect, the penalty is at least $1,000 per violation not to exceed $100,000 for all violations of the same requirement during the year.
- **Tier 3** – Where the violation is due to willful neglect but is corrected within 30 days, the penalty is at least $10,000 per violation not to exceed $250,000 for all violations of the same requirement during the year.
- **Tier 4** – Where the violation is due to willful neglect and is not corrected within 30 days, the penalty is at least $50,000 per violation not to exceed $1,500,000 for all violations of the same requirement during the year.

UPI will continue to collaborate with UCD to help promote faculty awareness of these new privacy and security regulations. Most notably, efforts are underway to provide education on the usage of
encryption software designed to secure PHI transmitted beyond the affiliate-protected email network. Encryption practices should be implemented immediately anticipating a September 2009 enforcement timeline.

FAQ's

What is Protected Health Information (PHI)?
PHI includes "individually identifiable" health information. Information is considered individually identifiable if (1) it identifies the individual or (2) there is a reasonable basis to believe that the information can be used to identify the individual. PHI can be more than just medical records and charts. PHI includes information relating to treatment, health condition, payment, MRNs, SSNs, and even simple demographic information, such as name, address and age.

What is the affiliate-protected email network?
The affiliate-protected email network includes UCD, UCH, UPI, TCH, BDC, DH&H and NJH. Security measures are already embedded within this network to ensure safe delivery of all email containing PHI. When sending email containing PHI outside of this protected network, you are required to utilize encryption software. The affiliate-protected network does not include emails originating from the Veterans Administration Hospital, patient/personal email accounts (ex. Hot-mail or G-mail), or private practice physician addresses outside of the affiliate network.

Why have we adopted email encryption practices?
Emerging HIPAA data security laws, coupled with growing privacy concerns and heightened liability, have necessitated the requirement that all communications containing PHI be secured. Encryption is a reasonable approach to securing confidential transmittal of PHI via email.

My patient is not technically savvy and may experience difficulty handling encrypted messages. Do I still need to encrypt?
YES. The encryption software utilized is not overly complex. Recipients will go through a few steps to access messages and will be able to respond securely as well.

My patient expresses no interest in secure email usage and they send unencrypted emails containing PHI to me all of the time. Why should I be concerned?
Implied consent cannot be assumed. When a patient sends an unencrypted email, it does not necessarily mean they are not concerned with secure information sharing. Many patients may not have the necessary tools to communicate securely via email. You can assist your patients by routing them through the encryption software. Additionally, you are required to send email securely even if the patient requests to opt-out from this practice.

I received an unencrypted email containing PHI from a referring physician outside of the affiliate-protected network. How should I respond?
Not all clinicians are aware of their responsibilities under the HIPAA data security and privacy laws. As a courtesy, you should remind the referring clinician they are placing their patient’s sensitive and personal information at risk for unauthorized access, modification, and disclosure. You should also encrypt this reply because PHI present in the original message is now part of the email thread.

How do I receive training on the usage of encryption software?
Information technology systems vary slightly from affiliate to affiliate. Encryption methods are dependent on your email address.

For staff utilizing UCD email, further guidance and detailed instructions on the use of encryption software is available by visiting:
http://administration.ucdenver.edu/admin/ts/securemail.htm

For staff utilizing UCH email, further guidance and detailed instructions on the use of encryption software is available by visiting:
http://hub.uch.edu/pdf/IS-Secure%20email.pdf

For staff utilizing UPI email, further guidance and detailed instructions on the use of encryption software is available by visiting:
http://intranet.upicololo.org/docs/IS/UPI-SAFEEmailEncryption.pdf

For staff utilizing TCH email, further guidance and detailed instructions on the use of encryption software is available by visiting:
http://email.thechildrenshospital.org:6300/psp/post/EMPLoyee/EMPL/e/?url=http%3a%2f%2fplanetch%2fdepartments%2findex.cfm%3frRecordID%3d40
By Colleen Ebel, Chief Information Security Officer
University of Florida College of Medicine
Chair, GIR Security Work Group, AAMC

As the stakes continue to rise for ePHI data breaches, academic medical centers (AMC) have embarked on what they formerly thought was an infeasible security control - encryption. Encrypted data transmission has not been a challenge with the availability of industry solutions such as SSL, TLS, SSH, VPNs and SSL VPNs. However, encryption of data at rest has vexed many IT organizations. Several states, and now the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule have put pressure on covered entities and institutions to encrypt their data. In September, the modified HIPAA rules require covered entities and their Business Associates to inform patients of any breach of their ePHI that is unencrypted.

The AAMC GIR security work group (GIR SWG) recently surveyed AAMC members on their data at rest encryption strategies. There were two parts to the encryption survey; policy and implementation. Ninety-three institutions responded to the survey answering questions about policy. Of the 93 institutions that responded, only 4 did not yet have some type of policy in place or in draft form for encryption of data at rest. Six of the 11 institutions that did not have an encryption policy in place or in draft cited lack of resources as the main reason.

Twenty-one institutions had an encryption policy in draft. Nine of those institutions cited lack of resources as the main reason their encryption policy was not yet in place (published and approved.) Four institutions indicated their policy was still in draft because their security policy body/committee had not made it a priority.

Seventeen institutions that responded to the survey had an over-arching institutional policy regarding encryption; however, specific types of data, data disposition, and media type were not specified. Local departments, divisions, or units were expected to decide for themselves.

Three institutions indicated they had a non-specific over-arching institution policy regarding encryption, but also had an encryption policy in draft. This suggests these institutions continue to evolve their policies as technology and user behaviors change. Perhaps the draft encryption policy for these institutions is intended to be more specific with respect to mobile computers and removable media.

Thirty-five institutions have put in place an institutional policy and/or standard on encryption of data at rest, and it includes requirements for specific data type, data disposition, and/or media type.

Twenty-six institutions cited the primary motivation for their policy work was the need for compliance with State/Federal regulations. Seventeen institutions cited their risk assessment as the main driver. Thirteen institutions indicated the primary motivation for their policy work was to implement common security practices. Only 12 institutions indicated an information security incident was their primary motivation.

In the second part of the encryption survey, institutions were asked about the implementation of their data at rest encryption strategy. Of the 93 institutions who responded to the survey, 55 had advanced their encryption of data at rest into implementation, 20 had not started implementing, and 18 refrained from answering the question about implementation. The most common strategy among institutions encrypting data at rest was encryption of laptops, removable media and backup tapes.

Encrypting data at rest has been a controversial security strategy. The effort to encrypt is significant and can be expensive. In addition, encryption can be destructive. As such, some covered entities had taken a wait and see approach.

However, the preliminary analysis by the GIR SWG of the encryption survey results indicate a strong trend among covered entities to move forward with encryption, particularly with mobile devices and media. The GIR SWG will publish a white paper in August containing a more comprehensive analysis of the survey results it received from the 93 AAMC members who responded to the survey.