MUNSON MEDICAL CENTER
MUNSON HEALTHCARE

Why

do I need to worry about encryption?

- The Department of Health and Human Services (HHS) issued this guidance “unsecure protected health information (PHI)" is essentially any PHI that is not encrypted or destroyed.” It does not matter how many chains, biometric devices or guards you have if it is not encrypted it is unsecure.
-
- HHS also introduced HITECH’s breach notification initiative. This requires any covered entity to follow pre-defined steps in the event of a breach. The steps depend on the scale of the breach however the use of encryption grants safe harbor in the event of a breach.

Who

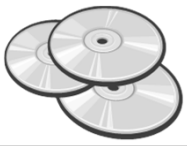
needs to know about encryption?

- All employees of a practice including providers need to know that encryption is required.
- Covered entities need to be informed of their requirements under the federal regulations.

What

examples can you provide?

- Email sent to a patient about their lab test results needs to be encrypted especially if the results are contained in the email.
- Files transmitted to appointment reminder services need to be encrypted.
- Websites for patient portals need to be secured E. g. https prefixes.
- CD's given to a patient with a copy of their medical record for a referral.



How can I comply?

- A simple policy requiring encryption of all data should be considered; the policy should address mobile devices.
- Software provided features such as Bit locker which is a component of Windows should be enabled and enforced for all devices and portable storage media.
  E. g. CD's and Thumb Drives.
- Periodic audits should be implemented.

When is the deadline?

- HHS does not require device encryption by a specified deadline.
- September 23, 2013 is the effective date for the breach notification initiative.

Where can I learn more?

- HHS classifies data into two categories:
  - Data at rest: data stored on laptops, hard drives, CD's, DVD's, Backup Tapes, servers.
  - Data in motion: data going thru networks including both wired and wireless networks.
- HHS does not provide guidance in the area of encryption.
- The National Institute of Standards and Technology (NIST) is a good source for a number of encryption publications.

National Institute of Standards and Technology

NIST National Institute of Standards and Technology U.S. Department of Commerce

Question and Comments

- Please feel free to contact me to discuss any security issue.
- Linda Bower
- SecurityOfficer@mhc.net
- 231-935-7619