HIPAA Breach Notification Rules
HITECH Act in ARRA

- Effective Sept 23, 2009
- Requires individuals and HHS to be notified if a breach of unsecured PHI occurs
- > 500 individuals = media notification
- Breach = Privacy Rule violation with potential harm to the individual
- Breach notification rules under further review
  - HHS may remove the “harm” threshold
Increased HIPAA Fines & Penalties

• Fines & penalties increased with graduated scales based on degree of negligence

• State Attorneys General now have HIPAA enforcement authority

• Mass. General fined $1M in 2011 for leaving patient information on subway in 2009

• Criminal penalties including imprisonment have been assessed for egregious acts
“Attorney General Darrell McGraw and CAMC Take Action to Resolve Security Breach that Exposed Information of 3655 Patients”

• Breach occurred at Charleston Area Medical Center Health Education Research Institute
• Patient information including SSN erroneously placed on the Internet; 94 hits
• Identified by the relative of a credit union employee, who notified the WV State AG

“Chapel Hill Researcher Fights Demotion After Security Breach”

Bonnie Yankaskas
PI, Carolina Mammography Registry
demoted from full professor to associate professor after one of 2 servers used by the Registry was hacked into in 2007, placing data, including SSN, on 180,000 women at risk

- Registry maintained for 15 years
- Hacked server not behind a firewall
“Researcher’s Demotion hurts UNC image”
Source: Newsobserver.com  Feb 3, 2011

127 researchers across the country sign petition backing Dr. Yankaskas for full reinstatement

“The image of UNC as being this place where smart, inquisitive people could conduct research with pride was huge. The fact they handled this in this way --- you couldn’t pay me a million bucks to work there.”

--- Dr. Patty Carney, Professor, Oregon Health & Science University
“Chapel Hill Researcher Fights Demotion After Security Breach”
Chronicle of Higher Education Oct 5, 2010

Who should be held accountable for a security breach?

**UNC Chapel Hill:** “Dr. Yankaskas is negligent in her university oversight duties for not ensuring the data was secure”; “University policies require data to be secure”

**Dr. Yankaskas:** “I am a scapegoat; University IT staffers knew the server was not behind the firewall in 2006 but didn’t tell me of the risk”; I’m not an IT expert”
Information Security

- We are all accountable for preventing information security breaches
  - PI’s are responsible for the security of the data generated in the research study

- Verify research data is stored securely—stay tuned for more information!!

- Develop research protocols with proper information safeguards ---
  - HIPAA office is available to review proposed protocols
Balancing Act

Too much security
System unusable

Too little security
System can be breached
Research

I don’t want to be an IT person..what do I do?

Follow the UNMC rules of the road

• Store your data on UNMC servers in the data center
• Have your server administered by an IT person
• If you have a need and the current products don’t meet your need, contact IT
Storage
UNMC has purchased additional Enterprise storage which is being implemented
UNMC issued an RFP for research storage
RFP’s being evaluated
Charging for storage being determined by Research Advisory Group
What is Security?

Those procedures and hardware that are employed to assure confidentiality of information

- Administrative
- Technical
- Physical
Defense in Depth

Identify assets to protect

Identify layers of protection

How do you protect your car

1. Take keys out
2. Lock the doors
3. Park in secure location
4. Use “club”
UNMC provides Infrastructure Security Layer
Defense in Depth: Network Layer
Defense in Depth

Trusted Network

DMZ

Internet Accessible Services

Video

Video Switch
Distance Education, Video Conferencing, and TeleHealth

Internet

VPN

Business Partners
Options for Research Data
Clinical Data Repository (CDR)
Use for Research

- Facilitate clinical research
- Reduce the need for detail chart reviews
- Consolidate research data in a centralized secure location
- Provide outcomes data to improve quality of care
CDR Oversight/Technical Assistance

Advanced Clinical Applications Program (ACAP):

- Byers Shaw, Jr. – Medical Director, 559-5565
- Hubert Hickman – Software Development, 559-3593
- Marsha Morien – Administrator, 559-4518

Stakeholders:

- UNMC
- TNMC
- UNMC-P
Information Security

General Rules of the Road
UNMC Rules of the Road

• Systems are to be used predominantly for University related business
• Highly recommend that you keep personal and work correspondence separate
• Demonstrate professional conduct when using email and voice mail systems
User ID or Login & Passwords

Individual logins must always be utilized to access confidential information.

Group logins are not permitted for access to confidential information.

You are responsible and accountable for access under your login.

1. Never post or share your login or password. (Except with IT for computer maintenance, then change it)
2. Never permit someone to use your computer while you are logged in
3. Use a strong password of at least 7 characters including numbers, and both upper and lowercase letters
User Privacy

• All traffic on the UNMC network can be monitored
• No user privacy is guaranteed
• Access to your email and files can be granted with authorization from General Counsel or Human Resources
Protect Yourself & UNMC Resources

1. Build strong passwords
2. Always log off a computer
3. Utilize screen savers with password displays so no one can use your computer when you are out of the area
4. Use of peer to peer protocol not allowed on UNMC network
5. Do not turn off security features on your workstation
   a. Anti Virus, anti spam, patch installation
Email and Internet Usage

• Be careful when replying to emails and where you go on the Internet
  1. “phishing”
  2. “tabnabbing”

• Verify you have correct email and fax numbers

• Do not send out mass emails
  1. Work with Public Relations
Social/Professional Networking

Do not disclose confidential information – including PHI, on MySpace, Facebook, Twitter, LinkedIn, etc.

Do not discuss patient care events, even if names or other identifiers are not used – it is still confidential.

Assignments on internal closed UNMC Blackboard sites are permitted.
Resources:

Information Security Plan

HIPAA Compliance Plan
Remember…

If you have questions or concerns about HIPAA Privacy or Information Security, or to report a suspected violation, call:

Sheila Wrobel, Privacy Officer @ 402-559-6767
Sharon Welna, Info Security Officer @ 402-559-2545
Deb Bishop, Compliance Specialist @ 402-559-5136