UNIVERSITY OF MINNESOTA

School of Nursing

Driven to Discover℠

School of Nursing Research Seminar

Data Security in The Academic Health Center

Presented By
Jon Harper – AHC Information Systems

UNIVERSITY OF MINNESOTA

School of Nursing

Driven to Discover℠

Overview of AHC-IS and Supported Services

- Provide desktop support to ~8500+ workstations/laptops (including Windows and Apple computers)
  - Includes support for over 5000 AHC faculty and staff (including select UMP and Fairview employees)
  - Limited support for tablets, phones, or other handheld devices
  - Does not include personally owned workstations or laptops

University of Minnesota
School of Nursing
Driven to Discover℠

Overview of AHC-IS and Supported Services

- Typical Services Provided For AHC-IS supported devices
  - Technical support via AHC-IS help desk
  - Walk-in technical support via the AHC-IS Tech Center located in Diehl Hall Bio-Medical Library
  - Assistance via remote sessions
  - Tier 2 on-site desktop support (i.e., hardware troubleshooting/repair, software installation/configuration, Email setup, workstation moves, and limited mobile device support)

University of Minnesota
School of Nursing
Driven to Discover℠

Overview of AHC-IS and Supported Services

- Typical Services Provided For AHC-IS supported devices (Cont.)
  - Hardware procurement, configuration, installation, and recycling
  - Laptop and workstation disk encryption
  - File storage/access and backup via AHC-IS managed servers
  - Respond to security incidents such as virus infections, suspected data breaches, or stolen devices

University of Minnesota
School of Nursing
Driven to Discover℠

Access to AHC-IS Support and Resources

- For AHC-IS Supported Users/Devices
  - Contact our help desk at 626-5100
  - Email ahc-is@umn.edu
  - Forms.ahc.umn.edu to request service
    - Data/File Server Access Request – add/modify/delete server access for an individual. Also used when someone leaves department
    - Request For Purchase – Request the purchase of computers, hardware, or software with University funds.
    - Add Existing Computer to Support – If a machine is added to support AHC-IS staff will configure it to comply with University policy

University of Minnesota
School of Nursing
Driven to Discover℠

Data Within the AHC

- Data Classification
  - Data within the AHC is classified as Private – Highly restricted
  - Units within the AHC have a security rating of “High”
  - Important to note as these classifications guide how data must be protected
  - Types of private data can include more than just patient data
  - For examples of public vs. private data see http://policy.umn.edu/operations/publicaccess-appc
  - For questions regarding specific types of private data or data you are responsible for, contact privacy@umn.edu

University of Minnesota
School of Nursing
Driven to Discover℠

Collaborating Inside/Outside the University

Only share private data with people authorized to view data via:

- Departmental Data Owner/Approver (for University employees)
- Data Usage Agreement (DUA)
  - Typically required by a data owner from a third party such as a healthcare provider
- Business Associate Agreement (BAA)
  - Contact privacy@umn.edu for questions about establishing a BAA with a third party provider, vendor, etc.

University of Minnesota
School of Nursing
Driven to Discover℠

Collaborating Inside/Outside the University (Cont.)

Current Methods to Share Data

- AHC-IS File Servers
  - Secure
  - Backed up nightly
  - Configured to comply with University policies regarding “Private – Highly Restricted” data
- Google Drive
  - Available to anyone with a University Gmail account
  - Sharing via the “Anyone with the link” option should not be used – too easy for accidental/unauthorized access
  - Store University private data only on a UMN Google Drive account
  - Google Drive should not be used to store PHI

University of Minnesota
School of Nursing
Driven to Discover℠

Collaborating Inside/Outside the University (Cont.)

Current Methods to Share Data (cont.)

- University Gmail
  - Email between UMN, UMP, and Fairview is considered secure
  - Private data (including PHI) should not be sent outside the University unless absolutely necessary
  - If private data must be sent via Email to someone outside the three organizations listed above, the data should be encrypted
    - Email is not encrypted by default; extra tools must be used to encrypt data before it is sent
  - In all cases regarding PHI, only the minimum amount of PHI necessary should be sent via Email.
  - For specific guidelines on sending PHI via Email see http://hub.ahc.umn.edu/sites/default/files/email-policy-protected-health-information.pdf
  - If you need further clarification contact privacy@umn.edu

University of Minnesota
School of Nursing
Driven to Discover℠

Collaborating Inside/Outside the University (Cont.)

- Currently, there is a gap at the University in being able to provide a compliant collaboration service with external entities
  - Netfiles, the current collaboration tool is being retired in April 2016; no new users are being added
  - Workarounds include sponsored accounts, encrypting data before sending to external entities, and in select cases providing remote access to AHC-IS file servers/data
  - OIT in conjunction with AHC-IS are working to implement a compliance based storage and collaboration service
  - Focus is on research that requires working with regulated data
  - Goal is to be compliant with various federal regulations (HIPAA, FISMA, etc.)
  - Scope is limited to smaller data sets (15-20 GB or smaller)
  - If you have a specific use case you feel can't be addressed contact AHC-IS and we will work with you to determine possible solutions

University of Minnesota
School of Nursing
Driven to Discover℠

Private Data Do's and Don'ts

Do's

- Save University data to a secure, AHC-IS managed file server
- Ensure devices accessing University private data are appropriately secured
  - AHC-IS supported devices meet University guidelines
- Use complex passwords to secure devices
  - Strongly consider creating passwords that exceed the minimum requirements
- Periodically review who has access to private data to ensure access is still appropriate
- Encrypt private data that is shared with external entities
- Encrypt external devices such as USB keys or hard drives if used to store private data

University of Minnesota
School of Nursing
Driven to Discover℠

Private Data Do's and Don'ts

Don'ts

- Store private data on non-University owned devices[1]
- Store private data on unencrypted workstations, laptops, or external devices[2]
- Use third party cloud services other than Google Drive to store private data
  - Dropbox, OneDrive, iCloud, etc.
  - These are not HIPAA compliant and there are no BAAs between these vendors and the University
- Post usernames/passwords on monitors or keyboards
  - This negates encryption completely
- Recycle/dispose of a device without proper sanitization[3]

1. Data Storage Standard
2. Device Encryption Standard
3. Media Sanitization Standard

University of Minnesota
School of Nursing
Driven to Discover℠

Mobile Devices in The AHC

What Is a Mobile Device

- A mobile device is defined as a tablet or smartphone that runs iOS or Android
- Users in the AHC are required to configure their mobile devices with additional settings than units outside the AHC

iOS Devices (Apple)	Android Devices
• 4 character numeric password, • Auto-locks after 15 minutes of inactivity • Requires passcode within 5 minutes of screen lock being enabled • Encryption is enabled (enabled by default when a passcode is set), • The user can issue a remote wipe command via iCloud, • Alternatively, 1-HELP can wipe the device if notified by the device owner.	• 4 character numeric password • After 10 incorrect password attempts, all data is erased and device is configured to factory defaults, • Auto-locks after 10 minutes of inactivity • The user can remotely reset the passcode, ring the phone, or wipe the device using http://www.google.com/apps/mydevices

University of Minnesota
School of Nursing
Driven to Discover℠

Mobile Devices in The AHC

Configuring a Mobile Device for UMN Gmail

- Setup guides for iOS devices are located at http://it.umn.edu/configure-ios-mobile-device-google-mail
  - You must choose “Exchange” as the account type
  - You must follow the additional instructions for members of the Health Care Component (HCC)
  - Once properly configured you will be required to configure a passcode
- Setup for Android devices are located at http://it.umn.edu/configure-your-android-device-sync-uofm
  - Once configured Google will prompt you to download an additional component
  - Once configured you will be required to configure a passcode
  - Encryption is not enforced do to the numerous variations of Android

University of Minnesota
School of Nursing
Driven to Discover℠

Mobile Devices in The AHC

Reminders

- If it is a personally owned mobile device it cannot store University private data
- If the device is lost or stolen the user should immediately contact AHC-IS (if they are supported by us) or 1-HELP to assist in performing a remote wipe of the device
- The user can initiate a remote wipe themselves if desired; instructions are in the email setup guides
- AHC-IS supported users can visit our walk-up tech center in Diehl Hall for assistance configuring mobile devices

University of Minnesota
School of Nursing
Driven to Discover℠

Portable Devices in The AHC

What Is a Portable Device?

- A portable device is defined as a USB key, external hard drive, CD/DVD, or memory card used to store data
  - If one of these devices will be used to store private data it must be University owned and should be protected via “hardware based 256-bit encryption”
  - Hardware based encryption is common for today’s external hard drives and USB keys, but verify before purchasing
  - Popular brands are Western Digital MyPassport for external drives; Kingston DataTraveler Vault or SanDisk Ultra Backup for USB keys
  - CDs/DVDs and memory cards do not support hardware based encryption
  - Once purchased you must still configure a passcode on the device for encryption to be active; encryption is only as good as your password

University of Minnesota
School of Nursing
Driven to Discover℠

Additional Resources

Useful Links

- AHC-IS Home Page
  - Provides greater details about services available
- AHC-IS Policies and Procedures
  - Particularly 3005E – Security Best Practices
- University Information Security Policy
  - Comprehensive; includes appendices a-v
  - Data classification policy - drives a number of compliance requirements
- Research Data Management Policy
- abuse@umn.edu
  - Report non-compliance, suspected security incidents, etc.

University of Minnesota
School of Nursing
Driven to Discover℠

Additional Resources (Cont.)

Stand Alone Encryption Products

- PGP (Pretty Good Privacy)
  - Link is to a YouTube tutorial; contact your local IT support if you're serious about using
  - Free (various versions)
  - Difficult to configure
  - Both parties must have application and certificates to decrypt data
- WinZip (Version 10+)
  - Simple
  - Must use paid version
  - Not FIPS 140-2 compliant
- Axcrypt
  - Free
  - Open source
  - Only 128-bit AES encryption

University of Minnesota
School of Nursing
Driven to Discover℠

Questions?

University of Minnesota
School of Nursing
Driven to Discover℠