IT Security Policy Review
Feinberg School of Medicine
18 July 2018
Threats to FSM Research Data

- Disrupted research & delayed patient benefits
- Diverted resources to address data breaches, investigations & audits, & corrective action plan will distract from core research mission
- Public/Internal embarrassment, negative publicity, reputation, furious patients
- Fines, penalties, financial expenses / losses (future/renewed grants)
- Intellectual property theft
- Phishing victim (e.g., ransomware)
- Lack of security training/awareness
Phishing

- Attempts to get you to do something or tell the hacker something private which may also compromise you or your computer in some way.
- Do not click on links – check on actual destination by hovering cursor over link.

- Avoid including sensitive information in email.
- Do not open attachments unless you explicitly requested it.
- Avoid propagating suspicious email by excessive forwarding.
- Check with IT support if unsure.
- Do not be curious!
FSM IT Security Policy Review

• Information Security & Access
• Data Security Plans
• Security Training
• Email Encryption
• Email Auto-forward
• File Sharing
• Device Security
Information Security & Access Policy

• September 22, 2016
• HIPAA/HITECH is the minimum standard for data handling
• De-identification must comply with the HIPAA Privacy rule
• Encryption is required (portable media, laptops, desktops, everything)
• Equipment, media, paper losses must be reported immediately
• Access to data must be maintained consistent with job role & approved IRB protocol
• Complex passwords are required
• Device security features are never to be disabled
• Research data on approved storage only (no Box.com, no Cloud)
• Use of commercial email systems are not permitted
• Data security plans are required
• Commercial vendors used in research require Dean’s office approval
• No non-public NU data on personal devices
• Policy: http://www.feinberg.northwestern.edu/it/policies/information-security/fsm-policy-security.html
• Questions & support, FSMIT-policy@northwestern.edu
Data Security Plan Policy

• Effective May 5, 2015, updated April 21, 2017
• Required for research of principal investigators with FSM appointments.
  - Plans are required for all new clinical research studies
  - Plans are required for existing studies at continuing review/renewal
  - Submission form triggered via FSM appointment declaration in the RSS Operational Data form
• Study focused risk assessment (e.g., data origination and flow, storage, access, backup).
• Checklist items for recruitments data sources, cloud storage
• All plans submitted to review (4608 as of 12/31/17) and audit (1086 as of 12/31/17).
• Built-in process improvement and vendor management
• Improves safeguarding of the University data
• Policy, template and examples:
  http://www.feinberg.northwestern.edu/it/standards-policies/information-security/index.html
• Questions & support, FSMIT-policy@northwestern.edu
CITI Program: HIPAA and Information Security Training (FSM)

• Collaborative Institutional Training Initiative (CITI) Program, www.citiprogram.org
• CITI Training can be accessed by anyone with a Northwestern NetID.
• Four modules, 3 required and 1 optional:
  Basics of Health Privacy (HIPAA) – Required
  Basics of Information Security, Part 1 – Required
  Basics of Information Security, Part 2 (includes Phishing) – Required
  Health Privacy Issues for Researchers – Optional
• Accessing the course:
  Go to www.citiprogram.org. Select “Log In”. Then select “Log In Through My Institution”. Click on “Northwestern University”. Enter NetID/Password. Then “Add a Course.” Scroll to Question 5 and enroll in the HIPAA, Security and Privacy Training course. Upon completion of the training, a certificate of completion will be logged in the CITI system and available to print.
Email Encryption Policy

- Effective October 1, 2015.
- Email message and attachments are required to be sent encrypted when containing PHI or PII.
- **Automatic Encryption** - Messages containing sensitive data sent from your @northwestern.edu e-mail address to or from recipients within Northwestern-affiliated domains are automatically encrypted and do not require additional effort. Northwestern-affiliated domains enabling automatic encryption:
  - northwestern.edu
  - cadencehealth.org
  - cdh.org
  - childrens纪念.org
  - lfh.org
  - livingwellcrc.org
  - luriechildrens.org
  - nmff.org
  - nmh.org
  - nm.org
  - northwesternmedicine.org
  - sralab.org
- **Manual Encryption** - Messages containing PHI or PII data sent from your @northwestern.edu e-mail address to non-Northwestern-affiliated environments will require manual encryption. Manually encrypted messages will be automatically quarantined.
- **Forced Encryption** - Email messages will be automatically encrypted and quarantined if manual encryption is not used and PHI or PII is suspected.
- Policy: [http://www.feinberg.northwestern.edu/it/policies/email.html](http://www.feinberg.northwestern.edu/it/policies/email.html)
- Questions & support, FSMIT-policy@northwestern.edu
Email Auto-forwarding Policy

- Effective October 1, 2015.
- Email message and attachments can be forwarded and/or auto-forwarded only within approved Northwestern-affiliated email systems. Current list published in policy.
  
  - northwestern.edu
  - cadencehealth.org
  - cdh.org
  - childrensmemorial.org
  - lfh.org
  - livingwellcrc.org
  - luriechildrens.org
  - nm.org
  - nmff.org
  - nmh.org
  - northwesternmedicine.org
  - sralab.org

- **Forwarding or auto-forwarding email messages and attachments to public email systems such as gmail.com, yahoo.com, or hotmail.com is not allowed.** * The use of public email systems are not approved for any research purpose at Northwestern University, Feinberg School of Medicine.

- Email systems fsm.northwestern.edu, u.northwestern.edu and md.northwestern.edu are Google public email systems and are not part of approved Northwestern-affiliated email systems for the exchange of research data and other sensitive information.

- Policy: [http://www.feinberg.northwestern.edu/it/policies/email.html](http://www.feinberg.northwestern.edu/it/policies/email.html)

- Questions & support, [FSMIT-policy@northwestern.edu](mailto:FSMIT-policy@northwestern.edu)

*Auto-forwarding will be disabled on the NU email system for FSM*
## FSM File Sharing Policy

<table>
<thead>
<tr>
<th>Data Type &amp; Examples</th>
<th>SharePoint</th>
<th>Vault (Research Only)</th>
<th>Northwestern File Servers</th>
<th>Google @u (Student Collaboration)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Public</strong></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>(e.g. calendar, course descriptions, maps, directory, approved census facts, audited financials)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Internal: Non-Sensitive</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>(e.g. meeting agendas, project documents, team building event)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Internal: Sensitive</strong></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>(e.g. salary plans, employment data, budgets, donor information, IRB data, CTEC, patent information)</td>
<td></td>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td><strong>Legally/Contractually Restricted</strong></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>(e.g. PHI, SSN, PII, student records, medical records)</td>
<td></td>
<td></td>
<td></td>
<td>No</td>
</tr>
</tbody>
</table>

Policy (NUIT): [http://www.it.northwestern.edu/file-sharing/overview.html](http://www.it.northwestern.edu/file-sharing/overview.html)
Questions & support, consultant@northwestern.edu

Policy (FSM): [http://www.feinberg.northwestern.edu/it/services/storage-options.html](http://www.feinberg.northwestern.edu/it/services/storage-options.html)
Questions & support, fsmhelp@northwestern.edu
Device Security Policy

- Effective April 15, 2016
- All devices: FSM IT managed & personal devices
- No non-public NU data on personal devices
- All devices must be encrypted and connection through only VPN
- Smartphones
  - Requires six-digit pin; and encryption enabled for Android devices
  - Limit of 30 days NU email
- Email synchronization to personal devices will be disabled on the NU email system for FSM
- Email synchronization via IMAP disabled
- Administrative rights will be phased-out
- Questions & support, FSMIT-policy@northwestern.edu
Information Security Policy References

Health Insurance Portability and Accountability Act (HIPAA):
http://www.hhs.gov/hipaa/for-professionals/index.html

Health Information Technology for Economic and Clinical Health (HITECH)

Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule:
http://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html

FSM Information Technology: http://www.feinberg.northwestern.edu/it/
FSM Email: http://www.feinberg.northwestern.edu/it/policies/email.html
FSM Storage Options: http://www.feinberg.northwestern.edu/it/services/storage-options.html
NU Storage Options: http://www.it.northwestern.edu/file-sharing/overview.html

Incident Response Protocol: http://www.it.northwestern.edu/policies/incident.html

NU Identity Management System (including passwords): http://www.it.northwestern.edu/auth-svcs/nuvalidate.html

Service Provider Security Assessments: http://www.it.northwestern.edu/about/departments/itms/cpo/assessment.html

NU Policies, Guidelines, and Practices: http://www.it.northwestern.edu/policies/
Secure IT at Northwestern: http://www.it.northwestern.edu/security/
Support & Resources (FSM)

• Central FSM IT Organization
  Carl Christensen, CIO
  Andrew Winter, Deputy CIO, Senior Director of Information Technology
  Carl Cammarata, Senior Director, Chief Information Security Officer
  Curtis Hanawalt, Director of Information Technology Customer Support
  open, Director of Information Technology Infrastructure
  Frank Schleicher, Director of Integrated Media Services

  FSM IT Steering Committee

• Central Support & Resources
  847-491-4357 or 1-HELP (from on campus)
  FSMHELP@northwestern.edu
  http://www.feinberg.northwestern.edu/it/index.html
Information Security Support & Resources

• FSM
  847-491-4357 or 1-HELP (from on campus)
  FSMIT-policy@northwestern.edu
  http://www.feinberg.northwestern.edu/it/standards-policies/information-security/index.html
  Carl Cammarata, Senior Director, Chief Information Security Officer, 312-503-2822
  David Gundrum, Senior Information Security Analyst, 312-503-3869
  Marvina Roebuck, Senior Information Security Analyst, 312-503-5735
  Leon Tran, Information Security Analyst, 312-503-6140

• University (Information & Systems Security/Compliance)
  847-491-4357 or 1-HELP (from on campus)
  security@northwestern.edu
  Thomas Murphy, Senior Director, CISO, 847-467-6422