Managing Information Security & Risk for FSM
Statistical Analyst and Biostatistician Seminar Series
January 10, 2017

Presented by
Carl Cammarata
Senior Director,
Chief Information Security Officer
Northwestern University
Feinberg School of Medicine

“We live in an age where you are private by effort and public by default”
Managing Information Security & Risk for FSM

Learning Objectives

• Why information security matters?
• What is at risk?
• What are our FSM information security policies – old and new?
• Our actions – what to do and not do?
Managing Information Security & Risk for FSM

FSM Support & Resources

• General IT Support
  Carl Christensen, CIO
  Andrew Winter, Senior Director of Information Technology
  Dong Fu, Director of Information Technology Infrastructure
  Frank Schleicher, Director of Integrated Media Services

  FSM IT Security Committee

  847-491-4357 or 1-HELP (from on campus)

  FSMHELP@northwestern.edu
  http://www.feinberg.northwestern.edu/it/index.html

• Information Security Support

  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
Managing Information Security & Risk for FSM

Why information security matters?

- Research participant privacy & security
- Research data integrity
- Sustain & grow research projects to improve human health
- Maintain healthy relationships with Covered Entity research partners
- Comply with regulations, contracts/grants criteria, University & FSM policy
- Stay out of the public eye, minimize OCR engagements, avoid fines & penalties

1- AFTERSHOCK PASSWORD BREACHES WILL EXPEDITE THE DEATH OF THE PASSWORD
2- NATION-STATE CYBER-ATTACKS WILL MOVE FROM ESPIONAGE TO WAR
3- HEALTHCARE ORGANIZATIONS WILL BE THE MOST TARGETED SECTOR WITH NEW, SOPHISTICATED ATTACKS EMERGING
4- CRIMINALS WILL FOCUS ON PAYMENT-BASED ATTACKS DESPITE THE EMV SHIFT
5- INTERNATIONAL DATA BREACHES WILL CAUSE BIG HEADACHES FOR MULTINATIONAL COMPANIES

Managing Information Security & Risk for FSM

What is at risk?

- 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

March 21, 2016
OCR Launches Phase 2 of HIPAA Audit Program

As a part of its continued efforts to assess compliance with the HIPAA Privacy, Security and Breach Notification Rules, the HHS Office for Civil Rights (OCR) has begun its next phase of audits of covered entities and their business associates. Audits are an important compliance tool for OCR that supplements OCR’s other enforcement tools, such as complaint investigations and compliance reviews. These tools enable OCR to identify best practices and proactively uncover and address risks and vulnerabilities to protected health information (PHI).

The audit program is developing on pace and OCR is committed to transparency about the process. OCR will post updated audit protocols on its website closer to conducting the 2016 audits. The audit protocol will be updated to reflect the HIPAA Omnibus Rulemaking and can be used as a tool by organizations to conduct their own internal self-audits as part of their HIPAA compliance activities.

To learn more about OCR’s Phase 2 Audit program, please visit our website at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html.

“Need to prepare, plan and implement an improved security and compliance posture.”
Feinstein Institute for Medical Research
$3.9 Million Settlement, March 16, 2016

“FIMR impermissibly disclosed the ePHI of 13,000 individuals when an FIMR-owned laptop computer containing ePHI was left unsecured in the back seat of an employee’s car. See 45 C.F.R. § 164.502(a).”

Corrective Action Plan
• 4 pages, 27 individual mandates
• Implementation reporting, annual reporting
  Public/Internal embarrassment, negative publicity,
  Intellectual property theft

One sub-item in the 27 individual mandates

“FIMR shall develop a complete inventory of all electronic equipment, data systems, and applications that contain or store FIMR ePHI, including personally owned devices.”

Managing Information Security & Risk for FSM

Case Studies - Exposed identifiable health and personal data

- ePHI data exposed to the Internet
- ePHI used in research without consent
- Unencrypted personal laptop stolen with ePHI in NU email
Managing Information Security & Risk for FSM

Policies – Old & New

Data Security Plans

Information Security & Access Policy (rewritten)

Research Use of EDW Data

Device Security Policy (new)

Email Encryption

Email Auto-forwarding

File Sharing

http://www.feinberg.northwestern.edu/it/standards-policies/index.html
http://www.it.northwestern.edu/file-sharing/overview.html
http://www.feinberg.northwestern.edu/it/services/storage-options.html
Managing Information Security & Risk for FSM – Data Security Plans

• Effective May 5, 2015.
• All NU IRB protocols for clinical research studies with principal investigator appointments at FSM now require a documented data security plan.
  - Plans are required for all new clinical research studies
  - Plans are required for existing studies at continuing review/renewal
• Plan will be submitted through the RSS of the IRB/RSS system.
• 13 questions (e.g., data access, data flow, data storage)
• 2270 plans reviewed, 668 audits (as of December 2016)
• Reduces data risk, increases compliance and security awareness
• Policy, template and examples: [http://www.feinberg.northwestern.edu/it/standards-policies/information-security/index.html](http://www.feinberg.northwestern.edu/it/standards-policies/information-security/index.html)
• Questions & support, FSMIT-policy@northwestern.edu
Managing Information Security & Risk for FSM – Research Use of EDW

- Effective May 5, 2015.
- Data recorded in Northwestern Medicine electronic medical records systems (e.g., EPIC, Cerner) for clinical care and desired to be used for research must be obtained from the Northwestern Medicine Enterprise Data Warehouse.
- Chart abstraction for research purposes or chart abstraction for clinical care purposes then later repurposed for research purposes is prohibited.
- Data not recorded in Northwestern Medicine electronic medical records system (e.g., EPIC, Cerner) but collected for research purposes such as patient reported outcomes and patient/family interview results conducted in a non-clinical care research setting are not in scope of this policy.
- Policy: [http://www.feinberg.northwestern.edu/it/standards-policies/research-use-of-edw-data.html](http://www.feinberg.northwestern.edu/it/standards-policies/research-use-of-edw-data.html)
- Questions & support, nmedwresearch@northwestern.edu
Managing Information Security & Risk for FSM – Email Encryption

- 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
  - lfh.org
  - nmff.org
  - cadencehealth.org
  - livingwellcrc.org
  - nmh.org
  - cdh.org
  - luriechildrens.org
  - northwesternmedicine.org
  - childrensmemorial.org
  - nm.org
  - ric.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
• 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
  - lfh.org
  - nmff.org
  - cadencehealth.org
  - livingwellcrc.org
  - nmh.org
  - cdh.org
  - luriechildrens.org
  - northwesternmedicine.org
  - childrensmemorial.org
  - nm.org
  - ric.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

*Auto-forwarding will be disabled on the NU email system for FSM*
## Managing Information Security & Risk for FSM – File Sharing

### Data Type & Examples

<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> (<a href="#">e.g. calendar, course descriptions, maps, directory, approved census facts, audited financials</a>)</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Internal: Non-Sensitive</strong> (<a href="#">e.g. meeting agendas, project documents, team building event</a>)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Internal: Sensitive</strong> (<a href="#">e.g. salary plans, employment data, budgets, donor information, IRB data, CTEC, patent information</a>)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Legally/Contractually Restricted</strong> (<a href="#">e.g. PHI, SSN, PII, student records, medical records</a>)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Last updated by NUIT, September 15, 2015

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](mailto: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](mailto:fsmhelp@northwestern.edu)
• Revision effective 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
Managing Information Security & Risk for FSM – 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 will also be disabled
- Administrative rights will be phased-out
- Device management technology being implemented
- Policy: http://www.feinberg.northwestern.edu/it/policies/information-security/index.html
- Questions & support, FSMIT-policy@northwestern.edu
Managing Information Security & Risk for FSM – Do’s and Do not’s

Please do

• Encrypt everything
• Store data on approved resources
• Backup your data
• Segregate data by study
• Maintain access to data consistent with IRB approvals
• Use complex passwords
• Leverage/use central FSM IT resources
• Adhere to policy

Please do not

• Use unencrypted media
• Store data on portable media
• Use unapproved cloud services
• Use vendors (even if free) without contracts
• Use commercial email services
• Disable security features

These are some points of emphasis from NU and FSM policy. It is not intended to be a comprehensive restatement of published policies.
Managing Information Security & Risk for FSM – Policy Resources

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

Feinberg Information Technology:  http://www.feinberg.northwestern.edu/it/


NUIT Policies, Guidelines, and Practices:  http://www.it.northwestern.edu/policies/

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

Secure IT at Northwestern:  http://www.it.northwestern.edu/security/

NU Validate: 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

File Sharing at Northwestern:  
http://www.it.northwestern.edu/file-sharing/overview.html

FSM Storage Options:  
http://www.feinberg.northwestern.edu/it/services/storage-options.html
Managing Information Security & Risk for FSM

• Knowing what to do is expected
• “Not knowing” is not OK
• “Not wanting to” is not OK
• Ask if you don’t know
• Everyone is responsible for data security

Lack of separation of responsibilities, management oversight and consequences of actions, excess access, mistakes, lack of training, non-compliance with policies and procedures, under utilization of existing security technology, laziness, convenience and covert activities increase data risks to the University.