Monthly Investigators Meeting
IRB Data Security Policy

Erik Decker
Assistant Director, Information Security
Personal Email: ed2513@mail.cumc.columbia.edu
Team Email: security@mail.cumc.columbia.edu

January 24, 2013
2012 BREACH OF PHI AND PII

- On Monday, October 15, 2012 a faculty member reported missing computer.
- Faculty member has dual hospital role and CUMC research role.
- Computer was not encrypted
- Back-up of computer data was available and analyzed.
  - 800,000 files -> 18,000 “notable” -> 39,000 duplicated patients -> 5000 unique patients
2012 BREACH OF PHI AND PII

• Approx. 5,000 individuals were notified that information related to their treatment and/or research was found in the computer files
  • CUMC research data 1,200
  • NYP patient data 3,600
  • NYP & CUMC faculty /staff 100

• Report to OCR – public webpage
• CUMC webpage notification
• Media notification
2012 BREACH OF PHI AND PII

• Meet reporting responsibilities and respond to patient inquiries

• Implementation of Endpoint Security Campaign
  • Encrypt all endpoint devices (desktop, laptop, phones etc)

• Walk up service for endpoint encryption at Helpdesk by Feb 1st, 2013

• Revision of Policies
  • Workstation Use Policy
  • Sanctions
  • Email Policy
  • IRB Data Security Policy
HOW DOES SYSTEM CERTIFICATION WORK?
Ongoing Discovery

2007-08 HIPAA Inventory
NYPH Interfaces
NYPH Data Warehouse Transfers
Meetings with Senior Leaders

Registration Policy / Self-Report
System/App Inventory
IRB

Assess (adopted HITRUST CSF)

Interview Sponsors
Interview System Custodians
Perform Vulnerability Scans

Report

Identify Risks
Define Impact
Make Remediation Recommendations

Remediate

Assist in Planning
Review Responses
Certify Implementation

One Year Review Cycle

Information Security Risk Management Program
## EXAMPLE RESEARCH SPECIFIC CONTROLS

<table>
<thead>
<tr>
<th>Category</th>
<th>Control ID</th>
<th>Question</th>
<th>Response</th>
<th>Comments</th>
<th>Help</th>
</tr>
</thead>
<tbody>
<tr>
<td>01-Access Control</td>
<td>01接入_01</td>
<td>Is there a documented departmental procedure for establishing, activating, modifying, revoking, disabling, and removing user accounts or do you comply with the CUMC EPHD Information Access Management and Control Policy?</td>
<td></td>
<td>The issue here concerns ensuring that only authorized users have accounts on research information systems. User accounts must be registered, tracked, and periodically checked. These processes, as carried out, must follow a documented procedure. This procedure must provide a mechanism for management control and oversight.</td>
<td></td>
</tr>
<tr>
<td>01-Access Control</td>
<td>01接入_02</td>
<td>Do the procedures require management approval before granting access rights to all users?</td>
<td></td>
<td>The issue here concerns ensuring that only authorized users have accounts on research information systems. User accounts must be registered, tracked, and periodically checked. These processes, as carried out, must follow a documented procedure. This procedure must provide a mechanism for management control and oversight.</td>
<td></td>
</tr>
<tr>
<td>01-Access Control</td>
<td>01接入_03</td>
<td>Are there documented procedures, which are actually carried out, for user registration, account tracking, and periodic review of user accounts?</td>
<td></td>
<td>Document your access control procedures for user registration and de-registration and include policies and procedures for establishing, activating, modifying, revoking, disabling, and removing accounts.</td>
<td></td>
</tr>
<tr>
<td>01-Access Control</td>
<td>01接入_04</td>
<td>Is management approval required for administrative level access?</td>
<td></td>
<td>The issue here is that special attention must be given to &quot;administrative&quot; accounts on systems. Management must review and approve all requests to grant administrative access privileges to a system. This process must follow a documented procedure.</td>
<td></td>
</tr>
<tr>
<td>01-Access Control</td>
<td>01接入_05</td>
<td>Is there a list of all users and their privileges?</td>
<td></td>
<td>You should maintain a list of all users and their access rights.</td>
<td></td>
</tr>
<tr>
<td>01-Access Control</td>
<td>01接入_06</td>
<td>Are users required to change passwords at least every 90 days?</td>
<td></td>
<td>Strong passwords are an important basic security measure.</td>
<td></td>
</tr>
<tr>
<td>01-Access Control</td>
<td>01接入_07</td>
<td>Are users prevented from reusing at least the previous 6 passwords?</td>
<td></td>
<td>Strong passwords are an important basic security measure.</td>
<td></td>
</tr>
<tr>
<td>01-Access Control</td>
<td>01接入_08</td>
<td>Are passwords required to be: at least 8 characters in length, not a word included in dictionaries; a combination of alphabetical upper and lower case characters and one special character?</td>
<td></td>
<td>The password settings must require passwords to be at least 5 characters in length, no dictionary words, upper and lower case with one special character.</td>
<td></td>
</tr>
</tbody>
</table>

Full list can be found at [https://secure.cumc.columbia.edu/cumcit/secure/security/sap.html](https://secure.cumc.columbia.edu/cumcit/secure/security/sap.html)
IRB CHANGES
NEW QUESTIONS

1) Does this study involve PII, which is inclusive of SSNs?

2) Does this study involve PHI or a Limited Data Set?

3) If there is PHI and/or PII that will be stored on a multi-user system, what is the System ID (next slide) number per the published CUMC IT Certified Environment List of the certified environment that your data are stored?

4) If there is PHI and/or PII, are all endpoint devices (including laptops, workstation, smartphones, tablets, flash drives, backup tapes, etc) storing these data encrypted and protected with a strong password, per the CU encryption policies?
# THE SYSTEM CERTIFICATION LIST

## Certified Systems as part of the Systems Certification Program

The list below is current as of January 14, 2013. Please see the System Certification Program page for a description of the program.

<table>
<thead>
<tr>
<th>System ID</th>
<th>System Name</th>
<th>Purpose</th>
<th>Department</th>
<th>Owner</th>
<th>System Classification</th>
<th>System Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>201</td>
<td>Medicare Patient DB</td>
<td>Research Project</td>
<td>Anesthesiology</td>
<td>Marlene D’Agostino</td>
<td>Research</td>
<td>Client/Server</td>
</tr>
<tr>
<td>228</td>
<td>Pediatric Anesthesia - ANQA</td>
<td>Research Project</td>
<td>Anesthesiology</td>
<td>Lena Sun</td>
<td>Research</td>
<td>Client/Server</td>
</tr>
<tr>
<td>7</td>
<td>CUMC/MSPH Secure Database System</td>
<td>Web applications and database servers for clinical trials and observational studies</td>
<td>Biostatistics</td>
<td>Seamus Thompson</td>
<td>Research</td>
<td>Client/Server</td>
</tr>
<tr>
<td>258</td>
<td>PC Recycling</td>
<td>Re-deployment of University computing assets for charitable causes.</td>
<td>Biostatistics</td>
<td>Norman Kleiman</td>
<td>Business</td>
<td>Workstation</td>
</tr>
<tr>
<td>304</td>
<td>Dean's Office Email Server</td>
<td>Mail Services</td>
<td>Biostatistics</td>
<td>Linda P. Fried, MD, MPH</td>
<td>Business</td>
<td>Client/Server</td>
</tr>
</tbody>
</table>

https://secure.cumc.columbia.edu/cumcit/secure/security/scp_systems.html
FURTHER EXPLANATION

• All PI’s must enter the “System ID” for any protocol (new or renewed)
  • Submissions with PHI/PII and not predetermined for certification will be returned to the PI.

• To certify a new or existing system contact Information Security
  • security@mail.cumc.columbia.edu
  • Risk Management has staffed up and is ready for your calls!
  • Certification does come with cost ($2000)

• Use of existing certified systems is encouraged
  • Look at the list and contact the System Owner

• IRB protocols will be audited for compliance with the new rules
  • COT will work with Information Security to ensure the submission of a System ID is accurate. Information Security will check with the System Owner.
EFFECTIVE DATE FOR MORNINGSIDE

• Policy released February 1st. Effective date August 1st, 2013.
  • New questions are in RASCAL now

• Register your system by going here:
  • https://secure.cumc.columbia.edu/cumcit/secure/security/sap.html

• System Certification List is published on a secure website
  • https://secure.cumc.columbia.edu/cumcit/secure/security/index.html
  • Those whose environments are certified and wish to host for other researchers please contact security@mail.cumc.columbia.edu. We will reflect this to aide investigators
Questions?
APPENDIX AND DEFINITIONS
PHI DEFINITION

Any information transmitted or maintained in any form (i.e., by electronic means, on paper or through oral communication) that relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual or the past, present or future payment for health care and (a) identifies the individual or (b) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual. Identifying characteristics of the identifier are listed below:
PHI 18 IDENTIFIERS

1) Names

2) All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code and their equivalent geocodes, except for the initial three digits of a zip code.

3) All elements of dates (except year) directly relating to an individual, including birth date, admission date, discharge date, date of death and all ages over 89 and all elements of dates (including year) indicative of such age, except for ages and elements aggregated into a single category of age 90 or older.

4) Telephone numbers

5) Fax numbers

6) Email addresses

7) Social security numbers

8) Medical record numbers

9) Health plan beneficiary numbers

10) Account numbers

11) Certificate/license numbers

12) Vehicle identifiers and serial numbers, including license plate numbers

13) Device identifiers and serial numbers

14) Web Universal Resource Locators (URLs)

15) Internet Protocol (IP) address numbers

16) Biometric identifiers, including fingerprints and voice prints

17) Full face photographic images or any other comparable images

18) Any other unique identifying numbers, characteristics or codes (other than unique codes assigned to code the data).
LIMITED DATA SET

Limited data set is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual: (1) names; (2) postal address information, other than town or city, State, and zip code; (3) telephone numbers; (4) fax numbers; (5) e-mail addresses; (6) social security numbers; (7) medical record numbers; (8) health plan beneficiary numbers; (9) account numbers; (10) certificate/license plate numbers; (11) vehicle identifiers and serial numbers; (12) device identifiers and serial numbers; (13) web URLs; (14) Internet Protocol (IP) address numbers; (15) biometric identifiers, including fingerprints and voiceprints; and (16) full-face photographic images and any comparable images.

Importantly, unlike de-identified data, protected health information in limited data sets may include the following: city, state and zipcodes; all elements of dates (such as admission and discharge dates); and unique codes or identifiers not listed as direct identifiers.
PII DEFINITION

Any information about an individual that could cause harm to such individual, such as medical, financial, employment or criminal records or other information, together with information that can be used to identify or trace an individual’s identity, including any other personal information that is linked or linkable to that individual. Examples include social security numbers, driver’s license numbers, and credit card numbers.