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
WHY?
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 will be 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)
  • Discovery by “boots on the ground”

• Revision of Policies
  • Workstation Use Policy
  • Sanctions
  • Email Policy
  • IRB Data Security Policy
ADDITIONAL REASONS

• Increasing regulation requires more mature processes
• Grant submission process should state use of certified environments
  • Data Security and Monitoring Plans (DSMP) can reflect this
  • Increases chances of grant awards in a future where federal funding is not growing
• In line with Dr. Lee Goldman’s “2020” strategic plan
  • “Be ‘pound for pound’ the best research-intensive medical school”
  • “Strengthen technology transfer and incentives to increase intellectual property”
WHO ARE WE?
Who is Information Security at CUMC?

- **Soumitra Sengupta**
  - Security Officer
- **Erik Decker**
  - Assistant Director
- **Rajneel Dhotre**
  - Security Manager
- **Lisa Mui**
  - Risk Manager
- **Michael Jemmott**
  - Analyst
- **Miguel Delgado**
  - Analyst
- **William Li**
  - Analyst
- **Achebe Sam**
  - Analyst
- **(Open)**
  - Analyst
- **(Consultants)**
  - Analyst
Information Security Program

System Certification Program

Security Governance
(Soumitra Sengupta, Erik Decker)

Security Operations
(Rajneel Dhotre)

Risk Management
(Lisa Mui)

Security Awareness
(Erik Decker)
CUMC Risk Management Program

- Pre-Implementation: Acquisition Analysis Complete
- Started: Analysis has commenced; questionnaire delivered to custodian
- To Be Issued: Report to be completed and/or released by Information Security
- Issued: Report has been released
- Remediation Escalated: Remediation has been escalated to senior management
- Remediation in Progress: Risk Mitigation plan accepted and/or activities have commenced
- Passed / Remediated: Remediation was completed or was not required
- Decommissioned: Application has been removed from service (post analysis) as a risk mitigation strategy
- Dropped: Applications thought to require certification but which do not
- To Be Started: Application risk analyses have not commenced

Total Applications: 501

Columbia University Medical Center
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, flash drives, backup tapes, etc) storing these data encrypted and protected with a strong password, per the CU encryption policies?
# SAMPLE SYSTEM CERTIFICATION LIST

<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>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>201</td>
<td>Medicare Patient DB</td>
<td>Research</td>
<td>Anesthesiology</td>
<td>Marlene D’Agostino</td>
<td>Research</td>
<td>Remediated</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>Remediated</td>
</tr>
<tr>
<td>7</td>
<td>SAC Data</td>
<td>Statistical Analysis for Clinical Trials</td>
<td>Biostatistics</td>
<td>Seamus Thompson</td>
<td>Research</td>
<td>Remediated</td>
</tr>
<tr>
<td>258</td>
<td>PC Recycling</td>
<td>Re-deployment of University</td>
<td></td>
<td></td>
<td>Business</td>
<td>Remediated</td>
</tr>
<tr>
<td>304</td>
<td>Dean’s Office Email Server</td>
<td>Mail Services</td>
<td>Biostatistics</td>
<td>Dr. Kleiman</td>
<td>Business</td>
<td>Remediated</td>
</tr>
<tr>
<td>311</td>
<td>ICAP Lab Database</td>
<td>HIV Related Services Program</td>
<td>Biostatistics</td>
<td>Chanon Gwynn, Deputy Director of M&amp;E</td>
<td>Research</td>
<td>Remediated</td>
</tr>
<tr>
<td>332</td>
<td>ICAP Website</td>
<td>HIV Related Services Program</td>
<td>Biostatistics</td>
<td>Chanon Gwynn, Deputy Director of M&amp;E</td>
<td>Research</td>
<td>Remediated</td>
</tr>
<tr>
<td>297</td>
<td>Mail Servers (6)</td>
<td>Mail Services</td>
<td>Center for Computational</td>
<td></td>
<td>Business</td>
<td>Remediated</td>
</tr>
<tr>
<td>380</td>
<td>MySQL Database</td>
<td>Data from CU data warehouse for lymphoid malignancy patients. Data also from WebCIS.</td>
<td>Center for Computational</td>
<td>Jose Morales</td>
<td>Research</td>
<td>Remediated</td>
</tr>
<tr>
<td>13</td>
<td>Study Manager</td>
<td>Patient Study Management</td>
<td>Clinical Trials Office</td>
<td>Rudina Odeh-Ramadan</td>
<td>FDA</td>
<td>Remediated</td>
</tr>
<tr>
<td>128</td>
<td>CURware</td>
<td>Research Pharmacy Database</td>
<td>Clinical Trials Office</td>
<td>Rudina Odeh-Ramadan</td>
<td>FDA</td>
<td>Remediated</td>
</tr>
<tr>
<td>15</td>
<td>Dental Mobile Van</td>
<td>Mobil Dental Van to See Patients</td>
<td>College of Dental Medicine</td>
<td>Stephen Marshall</td>
<td>Clinical</td>
<td>Remediated</td>
</tr>
<tr>
<td>252</td>
<td>ChemCart</td>
<td>Party Company-DeltaSoft, Inc.</td>
<td>Translational Immunology</td>
<td>Megan Sykes</td>
<td>Research</td>
<td>Remediated</td>
</tr>
<tr>
<td>28</td>
<td>Allscripts (Crown)</td>
<td>Enterprise EHR for Columbia Doctors</td>
<td></td>
<td></td>
<td>Research</td>
<td>Remediated</td>
</tr>
<tr>
<td>30</td>
<td>IDX</td>
<td>Centricity Business from GE</td>
<td>Columbia Doctors</td>
<td>Dr. Peter Stetson</td>
<td>Clinical</td>
<td>Remediated</td>
</tr>
<tr>
<td>32</td>
<td>Stockamp System</td>
<td>Trac/OnTrac</td>
<td>Columbia Doctors</td>
<td>Dr. Peter Stetson</td>
<td>Billing</td>
<td>Remediated</td>
</tr>
<tr>
<td>250</td>
<td>MD Audit</td>
<td>Compliance System</td>
<td>Columbia Doctors</td>
<td>Diane Yaeger</td>
<td>Business</td>
<td>Remediated</td>
</tr>
<tr>
<td>19</td>
<td>Sakai</td>
<td>Teaching Cases, NO patient data.</td>
<td>CUIT</td>
<td>Dr. John Zimmerman</td>
<td>Education</td>
<td>Remediated</td>
</tr>
<tr>
<td>34</td>
<td>Storage</td>
<td>Enterprise File Servers</td>
<td>CUMC IT</td>
<td>Robert De Boer</td>
<td>Business</td>
<td>Remediated</td>
</tr>
<tr>
<td>35</td>
<td>Exchange</td>
<td>Enterprise Email</td>
<td>CUMC IT</td>
<td>Robert De Boer</td>
<td>Business</td>
<td>Remediated</td>
</tr>
<tr>
<td>213</td>
<td>Matlab 2 aka RUBY</td>
<td>Clinical Data Mining</td>
<td>DBMI</td>
<td>George Hripcsak</td>
<td>Research</td>
<td>Remediated</td>
</tr>
<tr>
<td>214</td>
<td>Matlab 3 aka OPAL</td>
<td>Clinical Data Mining - to be retired in FY13</td>
<td>DBMI</td>
<td>George Hripcsak</td>
<td>Research</td>
<td>Remediated</td>
</tr>
</tbody>
</table>
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 ($$)

• Use of existing certified systems is encouraged (where appropriate)
  • 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

• TBD.  Looking for January 2013
  •  Dependent on changes to RASCAL

• There is still time to get your systems certified prior to policy enforcement – email us now!

• System Certification List will be published on 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?
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:
<table>
<thead>
<tr>
<th>PHI 18 IDENTIFIERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Names</td>
</tr>
<tr>
<td>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</td>
</tr>
<tr>
<td>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</td>
</tr>
<tr>
<td>4) Telephone numbers</td>
</tr>
<tr>
<td>5) Fax numbers</td>
</tr>
<tr>
<td>6) Email addresses</td>
</tr>
<tr>
<td>7) Social security numbers</td>
</tr>
<tr>
<td>8) Medical record numbers</td>
</tr>
<tr>
<td>9) Health plan beneficiary numbers</td>
</tr>
<tr>
<td>10) Account numbers</td>
</tr>
<tr>
<td>11) Certificate/license numbers</td>
</tr>
<tr>
<td>12) Vehicle identifiers and serial numbers, including license plate numbers</td>
</tr>
<tr>
<td>13) Device identifiers and serial numbers</td>
</tr>
<tr>
<td>14) Web Universal Resource Locators (URLs)</td>
</tr>
<tr>
<td>15) Internet Protocol (IP) address numbers</td>
</tr>
<tr>
<td>16) Biometric identifiers, including finger prints and voice prints</td>
</tr>
<tr>
<td>17) Full face photographic images or any other comparable images</td>
</tr>
<tr>
<td>18) Any other unique identifying numbers, characteristics or codes (other than unique codes assigned to code the data).</td>
</tr>
</tbody>
</table>
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.