Protecting Human Research Data: 
(Including Some Security Risks You Haven’t Thought Of)
Presented by

- **Thomas J. Moore, MD**, Associate Provost, BU Medical Campus and Executive Director, Office of Human Research Affairs (OHRA)
- **Arthur W Harvey III, MS, CPHIMS**, VP and Chief Information Officer at BMC
- **David Corbett, JD**, BUMC Information Security Officer
Data Breaches in Medical/Research

- A breach is an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information.

- Identifiable patient/research subject information
- HIPAA identifiers
Healthcare Data Breaches Are Common

Figure 1. Experienced a data breach involving the loss of patient data in the past two years
Data Breaches at Boston Hospitals (involving >500 records)

- 3 at Brigham and Women’s
- 2 at Beth Israel Deaconess
- 2 at Mass General
- 2 at St. Elizabeth’s

- *JAMA online April 3, 2017*
How do breaches occur?
Research Data Breaches Here at BUMC

- Hackers accessed older server containing research data
- Hackers accessed server with older security measures
- Hard drive stolen from a lab here at BUMC
- Student laptop stolen from student’s apartment (near miss)
- Utah.....
Preventing Breaches—Your Role

- Collect ‘minimum necessary’ data
- Secure your devices
- Train your people
- Know what resources BU and BMC can offer to help you
  - (Are you BU or BMC?)
What Can You Do to Avoid PHI Loss

- If you don’t need it, don’t collect it.
- Remove HIPAA identifiers

### HIPAA PHI “Identifiers”

<table>
<thead>
<tr>
<th>Left Column</th>
<th>Right Column</th>
</tr>
</thead>
<tbody>
<tr>
<td>Names</td>
<td>Certificate/license numbers</td>
</tr>
<tr>
<td>Geographic data (other than first 3 digits of zip code)</td>
<td>Vehicle identifiers and serial numbers including license plates</td>
</tr>
<tr>
<td>All elements of dates (other than the year)</td>
<td>Device identifiers and serial numbers</td>
</tr>
<tr>
<td>Telephone numbers</td>
<td>Web URLs</td>
</tr>
<tr>
<td>FAX numbers</td>
<td>Internet protocol (IP) addresses</td>
</tr>
<tr>
<td>Email addresses</td>
<td>Biometric identifiers (i.e. retinal scan, fingerprints)</td>
</tr>
<tr>
<td>Social Security numbers</td>
<td>Full face photos and comparable images</td>
</tr>
<tr>
<td>Medical record numbers</td>
<td>Any unique identifying number, characteristic or code</td>
</tr>
<tr>
<td>Health plan beneficiary numbers</td>
<td></td>
</tr>
</tbody>
</table>
Is Your Research Team Compliant?

- Assure that everyone with access to individually identifiable human subjects research data:
  - knows and complies with the security standards
  - accesses data on a secure device
Seek first to understand

- **BU Data Protection Standards**
  - Classify data (i.e, Public, Internal, Confidential, **Restricted Use**) and specify Minimum Security Standards

- **Section 40 on the BMC Policy & Procedure website:**
  - [http://internal.bmc.org/policy/](http://internal.bmc.org/policy/)
Store information securely

- Secure Network Storage for Restricted Use data
- Secure Cloud Storage: BU One Drive
- Special purpose applications
  - Redcap, Freezerpro
- Encryption on your laptop, phone/tablet, USB, CD/DVD
  - Enterprise (McAfee)
  - Personal (Bitlocker, FileVault)
- Personal phones/devices?
  - Must follow Minimum Security Standards
Transmit information securely

- Regular email Is Not Secure
  - Do not send data using BU email
  - Do not forward emails outside BMC

- Encrypt file or use BU SecureMail

- Connect securely using VPN when off-campus
Secure your devices - Minimum Security Standards

1. Pick a strong password/code - require at startup
2. Enable auto screen lock (5-15 min max)
3. Encrypt your device
4. Set Operating System and applications to automatically update
5. Install Antivirus, set to auto update and scan
Free software and services from BU

- Enterprise encryption for Windows and Mac
  - Crosstown Building (801 Mass Ave), Suite 485
  - bumchelp@bu.edu

- SecureMail

- Antivirus

- Off campus secure connect
  - [https://vpn.bu.edu](https://vpn.bu.edu)
Security Policies
Can be found on BMC Intranet at:
http://internal.bmc.org/policy/
Cover all aspects of information security
Includes forms to request security assessments

BMC Information Security Team
Can be reached through BMC Service Desk x44500
Can also be contacted through ServiceNow ticket
https://bmc.service-now.com/

Reporting
In the event of a suspect breach timely notification needs to be made to the BMC Privacy Officer Nickie Braxton
(Nickie.Braxton@bmc.org, 617-638-7987)

BMC-BU Relationship
Although we are tightly bound organizations, for the purposes of HIPAA security we are separate entities with separate policies
**HIPAA Definitions**

**Covered Entity**
- Health plans
- Health care clearinghouses
- Health care providers who conduct certain financial and administrative transactions electronically. These electronic transactions are those for which standards have been adopted by the Secretary under HIPAA, such as electronic billing and fund transfers.

**BMC IS a Covered Entity, BU IS NOT a Covered Entity**

Source: HHS.GOV
Business Associate
A person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information. Business associate functions or activities on behalf of a covered entity include claims processing, data analysis, utilization review, and billing. Business associate services to a covered entity are limited to legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services. However, persons or organizations are not considered business associates if their functions or services do not involve the use or disclosure of protected health information, and where any access to protected health information by such persons would be incidental, if at all. A covered entity can be the business associate of another covered entity.

Source: HHS.GOV
**HIPAA and Research**

**Researchers are typically NOT Business Associates**

To disclose protected health information to a researcher for research purposes, either with patient authorization, pursuant to a waiver under 45 CFR 164.512(i), or as a limited data set pursuant to 45 CFR 164.514(e). Because the researcher is not conducting a function or activity regulated by the Administrative Simplification Rules, such as payment or health care operations, or providing one of the services listed in the definition of “business associate” at 45 CFR 160.103, the researcher is not a business associate of the covered entity, and no business associate agreement is required.

MUST either have patient authorization or be using a limited data set

Source: HHS.GOV
But now the tricky bit....

BMC provides a full data set to a researcher who wants to do some initial screening and commits to reducing it to a limited data before it is “used” for research we have an issue. Absent patient authorization BMC is prohibited from releasing this data. If the researcher undertakes to create a limited data set out of the full data set they are providing one of the services specifically listed in the definition of “business associate” at 45 CFR 160.103 and as such become a business associate.

In order to avoid this issue only a limited data set can be provided from BMC which has implications for research.
Given the nature of BMC we assume that ALL data in our systems is PHI until proven otherwise.

Many different data items from different systems are considered PHI. This data is often communicated through internal systems and shared via internal documents for operational purposes. For those reasons the “security perimeter” at BMC is quite large. The following are examples of systems assumed to contain PHI:

- EHR and Clinical Systems
- Patient Accounting System
- Reimbursement System
- Email
- Shared file areas
- Every desktop, laptop, and USB drive
- Text messaging

Within this perimeter all data needs to be encrypted and monitored. No data should exfiltrate this perimeter without appropriate safeguards.
Why do we care?

Breaches are expensive
- Fines can run in the millions of dollars (Children’s Medical Center of Dallas - $3.2 million)
- Loss of reputation, most significant breaches involve at least some press coverage
- Opportunity cost, if we are spending time dealing with OCR we are not doing other important work
- It’s the law

Increased activity
- More aggressive enforcement, while not written in the regulation in practice OCR is taking a harder line on investigations and making routine demands for documentation
- Adding new threats, OCR has declared that ransomware attacks are now presumptively a breach and it is up to the covered entity to prove it is not a breach
- More social engineering attacks, PHI is valuable on the black market so there are more attempts to steal it
Q: How do bad guys usually get around security

A: They ask you to do it
Dear BU Employee,

Our new intrusion monitoring system that checkmates the increased incidents of phishing attacks and database compromise detected that your "BU" account was accessed from a blacklisted IP located in Arizona. Here are the details:

- **IP:** 23.19.88.141
- **Registered to:** Nobis Technology Group, LLC. Phoenix, Arizona
- **Time of compromise:** 8:17 AM, Eastern Standard Time (EST) -0500 UTC
- **Date of compromise:** Saturday, November 30, 2013

Did you access your account from this location? If this wasn't you, your computer might have been infected by malicious software. To protect your account from any further compromise, kindly follow these two steps immediately:

1. Follow this ITS secure link below to reconfirm your login details and allow the new IP monitoring alert system automatically block the suspicious IP (23.19.88.141) from further future compromise

   [http://netid-bu.edu/blockIP&malware](http://netid-bu.edu/blockIP&malware)

2. Update your anti-malware software and scan your PC immediately

With these two steps taken, your account will be secured.

Serving you better,
ITS and Database Security, Boston University
BU Web Login

BU login name

Password

Log In

Forgot Login or Password

Update Your Account | Web Login Help

View Mobile Version
Not Encrypted: no https

Not going to the real .bu.edu

Dark part of link is the real web server: “Msprotect-bu.edu”
The top part is controlled by your computer and the server.

The display window is completely controlled by the page author.
What the *new* weblogin looks like

Special Certificate shown in **Green:** Trustees of Boston University
No Green, No Go