HIPAA and
RESEARCH DATA SECURITY

Boston Medical Center and Boston University Medical Campus

January 2018

BOSTON MEDICAL CENTER
EXCEPTIONAL CARE. WITHOUT EXCEPTION.

BOSTON UNIVERSITY

This Training Will Cover-

What BU Medical Campus and BMC researchers need to know about HIPAA

What safeguards are required to keep personally identifiable health data used in research SECURE--whether covered by HIPAA or not

How to report a possible breach of research data

BOSTON UNIVERSITY

BOSTON MEDICAL CENTER
EXCEPTIONAL CARE. WITHOUT EXCEPTION.

Definitions

- **HIPAA**: The Health Insurance Portability and Accountability Act of 1996 (HIPAA). The regulations implementing the law contain Privacy, Security, and Breach Notification Rules
- **Covered Entity**: A health insurance plan, claim clearinghouse, or a healthcare provider that conducts HIPAA electronic billing (typically billing of insurance companies or Medicare/Medicaid). BMC is a Covered Entity
- **Covered Component**: Same as a Covered Entity, but is a healthcare component of an entity that does more than healthcare (a Hybrid Entity with designated Covered Components). BU is a Hybrid Entity.

More Definitions

- **Business Associates**: Persons/entities outside a Covered Entity that perform a service for the Covered Entity and need to access PHI. A Covered Entity or Covered Component must have a Business Associate Agreement with each business associate.
- **PHI**: Protected Health Information (PHI), which means information about an individual's past, present, or future physical or mental health, and information about payment for, or provision of healthcare services, created or received by a Covered Entity or Covered Component. HIPAA only protects PHI.
- **Treatment, Payment and Health Care Operations**: These are routine uses of PHI that do not require a patient Authorization. Any other purpose generally requires the individual's Authorization. Research requires an Authorization or an IRB Waiver of Authorization.

HIPAA and Research at BMC and BU

BU

- BU is a Hybrid Entity
- BU's Covered Components, subject to HIPAA, are the GSDM Dental Patient Treatment Centers; BU Rehabilitation Services; Sargent Choice Nutrition; and the Danielsen Institute.
- BU's professional schools (BUSM, SPH) are not Covered Components. PHI disclosed to them for research purposes (pursuant to a Waiver or Authorization) is not PHI

BMC

- BMC is not a Hybrid Entity.
- BMC is a Covered Entity under HIPAA.
- Whether you are caring for patients at BMC, doing research at BMC, or doing anything else with patient demographic or medical information-at BMC, it is PHI subject to HIPAA

When Does HIPAA Affect Human Subjects Research?

1. Recruiting subjects

2. Obtaining PHI/research data from HIPAA Covered Entity or Component

3. Protecting Your Research Data

1. Recruiting Subjects

HIPAA allows a treating provider to offer its own patients the opportunity to participate in research without an Authorization because discussing research participation with a patient is considered part of Treatment.

When submitting an application to the IRB for research approval, specify how you intend to recruit subjects. You may need a Waiver of Authorization, which the IRB may grant if you meet the qualifications for a waiver.

Qualifying for a Waiver for Recruitment Purposes

Research will qualify for a waiver for recruitment purposes if the PI can show the following:

(A) The use or of protected health information for recruitment purposes poses only a minimal risk to the privacy of potential subjects, because the researcher has:

> ***(1)*** An adequate plan to protect the patient contact information from improper use and disclosure;
>
> ***(2)*** An adequate plan to destroy the contact data identifiers at the earliest opportunity consistent with recruitment use (e.g., destroy identifiers of non-eligible patients and those who decline to participate); and
>
> ***(3)*** Adequate written assurances that the contact information used for research recruitment will not be reused or disclosed to any other person or entity, except as required by law and for authorized oversight of the research study, and;

(B) The recruitment could not practicably be conducted without the waiver; and

(C) The research could not practicably be conducted without access to and use of the protected health information for recruitment purposes.

BOSTON UNIVERSITY

BOSTON MEDICAL CENTER
EXCEPTIONAL CARE. WITHOUT EXCEPTION.

Researchers Outside BMC Recruiting BMC Patients

Let's say a researcher from MGH contacts BMC and asks for contact information of patients who may be eligible for his study, based on certain diagnoses. He does not need medical information, just contact information. Can BMC give him a list for study recruitment purposes?

- No, the list is PHI, even if it is only contact information, and cannot be given without an authorization or waiver. The list identifies individuals as patients of BMC.

HIPAA Compliant Study Subject Recruitment at Covered Entities where You Are Not On Staff

Options:

- Ask the unrelated Covered Entity to post information about the study and how to contact the study coordinator to participate, and wait until the subjects contact them.
- Ask a provider at the unrelated Covered Entity to give written recruiting material to potentially eligible patients so that they can contact your study staff on their own.

2. Obtaining PHI Data from a Covered Entity to Conduct Research

There are 4 pathways to obtain PHI from a Covered Entity for an IRB-approved research study:

1. Request only de-identified data from the Covered Entity
2. Request a Limited Data Set, under a Data Use Agreement
3. Get Authorization from each study subject
4. Obtain a Waiver of Authorization from the IRB

First Option: Obtain Only De-Identified Data

- PHI that has been "de-identified" is no longer PHI because it does not identify any individual.
- Note: de-identification under HIPAA does not mean simply deleting the patient names. HIPAA regards data as de-identified only in two circumstances:
  - If the data does not contain any of the 18 identifying elements (next slide), or
  - If the data contains some of those 18 identifying elements, but an expert has determined there is a very small risk of using the data to identify individuals. If you wish to pursue an expert determination, contact the BU Privacy Officer at hipaa@bu.edu so she can assist in ensuring the expert uses methods advised by HIPAA.

18 Identifiers That Must Be Absent To De-identify PHI

- Names
- All geographic subdivisions smaller than a State
- All elements of dates (except year) for dates directly related to an individual:
  - birth date
  - admission date
  - discharge date
  - date of death
  - all ages over 89
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social Security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers, e.g., serial numbers, license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images
- ***Any other unique identifying number, characteristic, or code***

BOSTON UNIVERSITY

Second Option: Obtain Only a Limited Data Set

- Do not have to remove *<u>all</u>* 18 identifying elements. Can leave the following:
  - town or city and zip code of subject
  - dates related to the subject, e.g., dates of birth, death, admission, testing, etc.
- The Covered Entity will require a Data Use Agreement

Third Option: Obtain Patient Authorization

- Researchers can obtain PHI from BMC or another Covered Entity if subjects sign a HIPAA authorization
- The HIPAA Authorization is often combined with the study Consent

- *Practice tip* - Identify all covered entities whose records you will be seeking and name each in the Authorization

Fourth Option: Obtain IRB Waiver of Authorization

If patient Authorization is not possible or practical, such as in a retrospective review of records, the researcher can request a Waiver from the IRB, if:

- PHI is necessary for the research,
- The research cannot be conducted without a waiver; and
- The research does not involve more than a minimal risk to individuals because you have:
    - An adequate plan to protect the identifiers from improper use
    - An adequate plan to destroy identifiers at the earliest opportunity
    - Assurance that the PHI will not be used for any purpose other than that study, and it won't be further disclosed

SAFEGUARDS

HIPAA and More

Depending on the type of data involved, a number of statutes require researchers to protect research data, and many impose serious penalties for breaches:

- HIPAA
- Massachusetts Standards for Protection of Personal Information (93H / 201 CMR 17)
- Payment Card Industry Data Security Standard
- Export Control Law
- Controlled Unclassified Information (32 CFR Part 2002)
- Human Subjects and other research regulations

See BU Data Protection Standards

BU and BMC Minimum Security Standards

BU and BMC Policies require Minimum Security Standards for all non-public data

- http://www.bu.edu/policies/information-security-home/data-protection-standards/minimum-security-standards/
- http://internal.bmc.org/policy/

All devices and data storage used for human subjects research, and all electronic sharing of non-public research data
must comply with these standards

Classification of Non-Public Data at BU and BMC

BU

Restricted Use: loss/misuse may require notification to individuals or government agency –

- PHI and personally identifiable health data used in research
- Code or key to re-identify data

Confidential: loss or misuse may adversely affect individuals or BU business

- non-health research
- De-identified PHI/health data

Internal: potentially sensitive

BMC

Confidential: disclosure may cause serious harm

- Includes both PHI and personally identifiable health data used in research

Internal: disclosure may cause some harm

Slightly different nomenclature;
Same minimum standards for non-public data

Bottom Line on Protecting Research Data

If you are using *public* data, and if you are not concerned about your research becoming *public*, you do not need to worry about these safeguards and standards

If your data or your research is non-public, you must implement the device safeguards and observe the safeguards applicable to sharing and data storage

The highest level of protection applies to research data that may be used to identify an individual (alone or in combination with other data) -- PHI or not.

What’s The Big Deal?

At Feinstein Institute for Medical Research, an *unencrypted laptop* was *stolen from a car*, containing data of about 50 research studies and approximately 13,000 individuals

- *Big money payment*: settled alleged HIPAA violations for ***$3.9 million***
- *Ongoing government scrutiny:* three year corrective action plan
- *Loss of confidence and reputation*: required to notify research subjects and media outlets

Yes, This *Could* Happen to You

- NYU School of Medicine Aging and Dementia Clinical Research Center, 2010: *Unencrypted portable device* with information of 1,200 was *lost*
- Kern Medical Center, 2012: Bag containing *paper records* of 1,500 (including HIV, AIDS, Hepatitis, and pregnancy test results) was *stolen* from a car
- Oregon Health and Science University, 2013: Surgeon’s *unencrypted laptop was stolen* from a vacation rental; $2.75 million settlement with OCR
- U Conn, 2016: *Malware* exposed research data on servers
- NY State Psychiatric Institute, 2016: *Hackers* accessed servers with highly sensitive information of 22,000 individuals participating in mental health studies

A Clear Pattern:

Lost or Stolen:

- *Unencrypted* laptop
- *Unencrypted* portable device (e.g., flash drive)
- Paper or other tangible research data

Cyberattack

- Malware
- Phishing attack
- Exploit of operating system or application vulnerabilities

<u>We may not be able to prevent all breaches, but following the rules on the following slides will prevent most!</u>

BOSTON UNIVERSITY

Summary of BU/BMC Data Protection Standards

Electronic Data

1. Device Standards
2. Device Hygiene
3. Data Storage
4. Data Backup
5. Secure Email
6. Fight Phishing
7. Working Remotely

Non-Electronic Data

8. Protecting Verbal Data
9. Protecting Tangible Data
   - Paper
   - X-rays
   - Other tangible forms

1. Device Standards

All endpoint devices - such as desktops, laptops, and phones - must have:

- Operating systems and applications that are supported and updated
- Anti-Malware installed and set to auto update and scan
- Auto screen lock (15 min max) to password/code
- Disk encryption (BMC – required / BU - only required for Restricted Use data)

Note: Your personal devices are not affected *unless* used to access, process, or store research data.

BOSTON UNIVERSITY

BOSTON MEDICAL CENTER
EXCEPTIONAL CARE. WITHOUT EXCEPTION.

BMC And BU Are Here To Help!

Do what you can with the guidance found here:

http://www.bu.edu/tech/support/information-security/securing-your-devices/

Ask for help:

BUMC IT Help: http://www.bumc.bu.edu/it/support/bumc-it/request/

BMC ITS Service Desk: https://bmc.service-now.com/

2. Device Hygiene

Keep operating systems and applications up to date, by enabling auto-update or promptly updating when notified

Periodically change your strong password, following best practices: http://www.bu.edu/tech/about/security-resources/bestpractice/passwords/

Regularly delete files when no longer needed, including emails and downloads

3. Data Storage

BU

Restricted Use Data Storage:

- BU network storage
- BU Microsoft SharePoint or OneDrive
- BU Dropbox (not HIPAA data)

Confidential Data Storage:

- All of the above, plus:
- BU Google Drive

BMC

PHI storage

- Any BMC network, to share with those who also have access
- Box.com

4. Data Backup

You should have a backup plan, and be careful where you store the data:

- At **BU** use approved tools and storage options. BU network storage comes with a backup plan: http://www.bu.edu/tech/support/storage-options/
- At **BMC** use network storage or a Box.com account
- Use only encrypted devices: removable media (e.g., CD, DVD, USB key/stick) must be **encrypted & password protected**.

5. Secure Email

BU Email

BU email does not have encryption –

- Use Data Motion to send Restricted Use data securely, both
  - within BU (xxx@bu.edu to yyy@bu.edu) and
  - to non-BU addresses (including to yyy@bmc.org)

BMC Email

BMC Email:

- Within BMC (from a xxx@bmc.org to yyy@bmc.org) is considered secure, so long as no non-BMC addresses are included
- Remember- emails may always be forwarded. Consider adding warning to email
- Outside BMC: type “secure” in the subject line to encrypt & send only to HIPAA secure addresses

Secure alternative: Use regular email, but encrypt the document or spreadsheet:

- Encrypt when you save the document or spreadsheet, then attach to email
- Provide the password to the recipient by telephone
- Do not send the password by email because it maybe intercepted
- Do not put RU data in subject line or body of email

6. Fight Phishing!

- Most people think it would never happen to them, but attempts are made *regularly* at BU and BMC. **Red Flags:**
  - Email asks for password – BMC and BU will never ask for login credentials through email
  - Sense of urgency and not expected
  - Grammatical/spelling errors
- If there is any doubt, please get advice:

BU email: forward the email to abuse@bu.edu . Learn more at our "How to Fight Phishing" webpage: http://www.bu.edu/tech/services/cccs/email/unwanted-email/how-to-fight-phishing/	**BMC email:** **DG-Spam-attack@bmc.org**

Check Before You Click

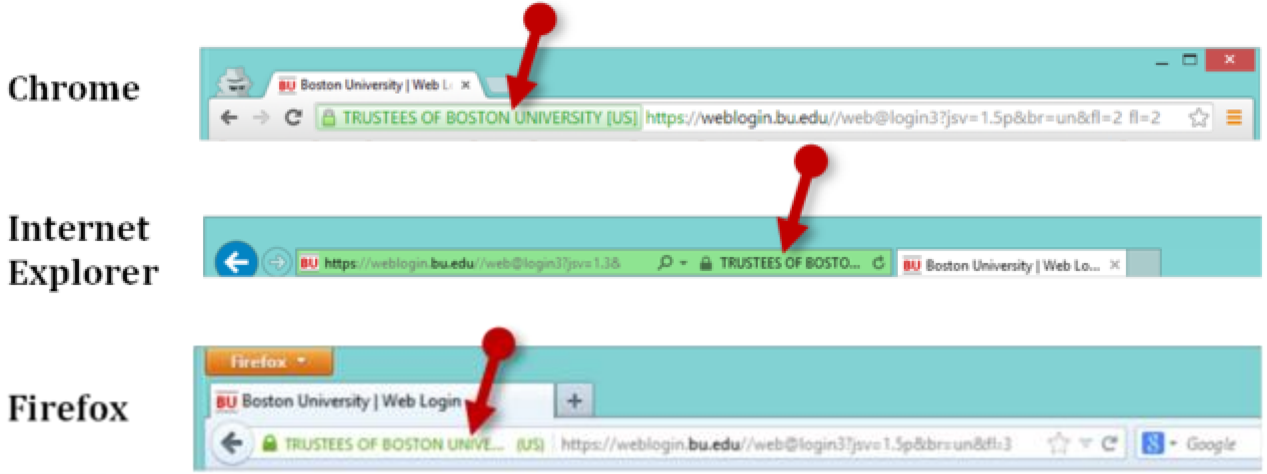
- Context
  - Did you expect this email?
- Sender
  - Verify address is bu.edu, not b0.edu, b1.edu or something else
- Links
  - Hover over links to verify

> On Jan 2, 2018, at 12:31 PM, Corbett, David <corbettd@bx.edu> wrote:
>
> Hello Bob,
>
> Don’t miss out on your free trial.
>
> Your free access ends tonight at midnight.
>
> Lets meet for lunch this Tuesday, on me,
>
> David

Check Before You Type Your Password

Websites

- Only enter login credentials if website address has **green** component (EV Cert) and starts with https://
- Without the "s" preceding the colon, the website is not safe
  - Learn more at our "How to Fight Phishing" webpage


Chrome
Boston University | Web L
TRUSTEES OF BOSTON UNIVERSITY [US]
https://weblogin.bu.edu//web@login3?jsv=1.5p&br=un&fl=2 fl=2
Internet Explorer
https://weblogin.bu.edu//web@login3?jsv=1.38
TRUSTEES OF BOSTO...
Boston University | Web Lo...
Firefox
Firefox
Boston University | Web Login
TRUSTEES OF BOSTON UNIVE... (US)
https://weblogin.bu.edu//web@login3?jsv=1.5p&br=un&fl=3
Google

7. Safeguards For Working Remotely

Use BMC secure remote access (https://mybmc.org or https://portal.bmc.org) or the BU VPN (vpn.bu.edu); otherwise, even passwords can be intercepted and viewed

Do not leave devices unattended (e.g., coffee shops, cars)

Lock up devices when not in use (e.g., cable lock, locked room)

8. Verbal Safeguards

- Do not discuss individual participant data outside closed offices
  - If necessary, talk quietly and away from others

- Play music or background noise to disguise conversations

- If necessary to contact friends/family to locate a research participant, only disclose the minimum necessary amount of information

9. Safeguards For Documents and Tangible Data

Do not remove documents or tangible data from the office

If you must, don't leave unattended (e.g., car, classroom, coffee shop)

Lock up when not in use

Shred when no longer necessary – never throw in trash

BREACHES:
What are they?
How do I report?

Reporting Potential Breach/Loss of Data: Why Is It So Important?

BMC/BU may have an obligation to report the incident to individuals, the IRB, or state and federal authorities

BMC/BU may be able to prevent or minimize damage

Please note that any external reporting to governmental agencies or individuals whose data has been breached is handled by BMC/BU HIPAA Officers and other offices. Your responsibility is to report any suspected security incidents to irt@bu.edu or privacy@bmc.org and assist as requested in any investigation.

BOSTON UNIVERSITY

BOSTON MEDICAL CENTER
EXCEPTIONAL CARE. WITHOUT EXCEPTION.

What Events Must Be Reported?

Unusual system activity, including:

- Malware detections
- Unexpected logins
- System or application alerts indicating a problem
- Unusual behavior such as seeming loss of control of mouse or keyboard

Unauthorized access, use, disclosure, or loss, including:

- Loss of a device (personal or BU-owned) used to access research data
- Loss of tangible (paper or other) research data
- Emailing without encryption

How to Report Security Concerns, Security Incidents, and Potential Breaches

If you think the data belongs to BU, send an email to BU's Incident Response Team (IRT): irt@bu.edu IRT will triage the report and contact the appropriate persons and offices

If you think the data belongs to BMC, send an email to BMC's Privacy Officer: privacy@bmc.org

Wherever you report to- BMC or BU—we will ensure the report gets to the appropriate person at either/both

BMC and BU prohibit retaliation for reporting security concerns, security incidents, and potential breaches

Additional Resources on HIPAA and Data Protection

- This PowerPoint is available at www.bu.edu/hipaa
- BU Data Protection Standards: http://www.bu.edu/policies/information-security-home/data-protection-standards/
- BMC Policies: http://internal.bmc.org/policy/
- BMC HIPAA Privacy Officer: privacy@bmc.org
- BU HIPAA Security Officer David Corbett: corbettd@bu.edu
- BU HIPAA Privacy Officer Diane Lindquist: dlindq@bu.edu
    - Both receive emails at this address: hipaa@bu.edu
- NIH education materials https://privacyruleandresearch.nih.gov/clin_research.asp