HIPAA & RESEARCH DATA SECURITY FOR BU RESEARCHERS

CHARLES RIVER CAMPUS

November 14, 2017

BOSTON UNIVERSITY

This Training Will Cover-

- How HIPAA impacts human subject research

- What researchers need to do to protect health data used in research - whether covered by HIPAA or not

- How to report a possible breach of research data

- Your BU resources

BOSTON UNIVERSITY

HIPAA

Health Insurance Portability and Accountability Act of 1996 (HIPAA).

- Privacy
- Security
- Breach Notification
- Patient Rights

What’s the big deal?

- National standards
- Complexity
- Enforcement: consequences of breach
  - Feinstein Institute for Medical Research: data from 50 studies, 13,000 individuals; breach cost $3.9 million
  - Oregon Health and Science University, $2.75

BOSTON UNIVERSITY

When Research Implicate HIPAA?

Human subjects research

Using PHI

Protected Health Information (PHI):

- Information about an individual’s past, present, or future physical or mental health, and/or
- information about payment for, or provision of healthcare services,
- created or received by a Covered Entity/Covered Component.

Covered Entity/Covered Component

- **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).
- **Covered Component**: Same as a Covered Entity, but is a component of a hybrid entity that does more than healthcare. BU is a Hybrid Entity.
- **BU Covered Components**:

GSDM's Dental Health Treatment Centers

SAR Physical Therapy and Neuro-Rehabilitation

Sargent Choice Nutrition

Danielsen Institute

Research examples: Is HIPAA Implicated?

1. Research involving analysis of stillbirths and mothers age. Using birth and death statistics from public records.
2. Same research study, but also uses data from BMC
3. What modality is most effective in treating major depression plus anxiety: CBT, meditation or both? Data from:
   - Meditation center
   - Reported by subjects
   - BU CARD
   - Danielsen Institute

BOSTON UNIVERSITY

Points Where HIPAA Matters

1. Preparing proposal

2. Recruiting subjects

3. Obtaining data

4. Protecting your data

HIPAA in First Phase of Research: Preparations (Pre-IRB Submission)

You need PHI from a BU Covered Component (or from a HIPAA Covered Entity outside BU) to prepare for research. For example:

- Evaluating whether the medical records contain enough potential subjects for a research study
- Obtaining other information from medical records to prepare the proposal or IRB submission
- Designing a research proposal or protocol

Two options: Authorization or Waiver

Waiver Preparatory To Research

- **Patient Authorization**: usually impractical
- **Waiver Preparatory to Research** if:
  - Review of PHI is necessary to prepare the protocol or engage in similar preparatory activities;
  - The researcher will not remove or retain the PHI reviewed; and
  - Reviewing the PHI is necessary for research purposes
- If you want to review data at a BU covered component, use the form available at www.bu.edu/hipaa and give it to the covered component's HIPAA Contact.
  - Practices vary at health care providers outside BU - start by asking for the Privacy Officer
- Why is this necessary? Accounting

HIPAA in Second Phase of Research: Recruiting Subjects

- A treating provider can offer its own patients the opportunity to participate in research. Discussing research participation with a patient is considered part of Treatment; so no Authorization or Waiver is needed.

- It doesn't matter that the researcher does not personally treat each potential study subject; the clinic is considered the provider.

BOSTON
UNIVERSITY

HIPAA-Compliant Recruiting Examples

A physical therapist who is part of BU Physical Therapy at the Ryan Center has IRB approval to conduct a study comparing two post-knee surgery treatment regimens. Can she review patient records to get contact information for potential subjects and contact them about the research?

Same research is being conducted by a researcher at Northeastern University. Can BU Physical Therapy give him that list for study recruitment purposes?

HIPAA in Third Phase of Research: Obtaining PHI from Covered Entity to Conduct Research

- There are 4 pathways to obtain PHI from a Covered Entity for an IRB-approved research study:
  - Request only de-identified data from the Covered Entity
  - Request a Limited Data Set, under a Data Use Agreement
  - Get Authorization from each study subject
  - Obtain a Waiver of Authorization from the IRB

First Option: Use De-Identified Data

- PHI that has been "de-identified" is no longer PHI because it does not identify any individual.
- But 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.

BOSTON UNIVERSITY

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: Use a Limited Data Set

- Do not have to remove *all* 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.
- Must enter into a Data Use Agreement with the Covered Entity that specifies how you will protect and use the data
- If you wish to pursue this method, contact the BU Privacy Officer at hipaa@bu.edu

Third Option: Obtain Patient Authorization

- Researchers can obtain PHI from a Covered Entity or BU covered component if subjects sign a HIPAA authorization
- The HIPAA Authorization may be combined with the study Consent, or it may be separate
- Practice tip - Identify all covered entities whose records you will be seeking and name each in the Authorization

Fourth Option: IRB Waiver of Authorization

Conditions for granting a Waiver:

- PHI is necessary for the research,
- The research cannot be conducted without a waiver (usually because obtaining individual Authorization is impractical) and
- The research does not involve more than a minimal risk to individuals based on the following:
  - 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

4. Protecting Your Research Data

Major Risks:

- Lost or Stolen:
  - Laptop
  - Portable device (e.g., flash drive)
  - Paper or other tangible research data

- Cyberattack
  - Malware
  - Phishing attack
  - Exploit operating system, application vulnerabilities

HIPAA Is Not The Only Law Out There…

Many laws may protect your human subjects research data, for example:

- 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, and
- HIPAA

PHI or Not During Research?

Subject enrolls in depression/anxiety study. Researchers collect the following. Which are PHI?

- Subject records moods daily for a month.
- Subject provides Authorization for release of her records from Danielsen
- Subject provides Authorization for release of her records from CARD
- Subject provides Authorization for release of her records from meditation center

BU’s Data Categories Make it Simple[r]

- Restricted Use: loss/misuse may require notification to individuals or government agency –
  - HIPAA PHI and other 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
  - Human subjects research with non-health data (e.g., College of Arts and Sciences investigating whether pre-teen music lessons impact academic success)
  - De-identified PHI/health data
- Internal: potentially sensitive
- Public: does not require protection from disclosure

But my research data is always “deidentified”….

- Are you sure?
- That means your data has no dates and no geographic signifiers, or any of the 18 elements listed in HIPAA
- **<u>And</u>**, that no one can identify an individual from your data– either alone or in combination with other available data.

Cautionary tale: Iowa insurance executive:

“Health costs are skyrocketing! It costs $1 million per month to cover treatment for one 17 year old boy’s with hemophilia.”

Minimum Security Standards for Non-Public Data

The BU Data Protection Standards identify Minimum Security Standards for all non-public data (Restricted Use, Confidential, and Internal)

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

4 Easy Rules

1. Device standards
2. Data storage options
3. Data sharing options
4. Foil Hackers

1 Big Theme

ENCRYPT!

1. Device Standards for Non-Public Data

- Devices = desktops, laptops, and phones
- Devices 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** (best practice but required for Restricted Use data)

Note:
Your personal devices do not need to meet these standards ***unless*** you use them to access, process, or store research data.

BOSTON UNIVERSITY

How Do I Make Sure my Device is OK?

- BU has guidance here:
  - http://www.bu.edu/tech/support/information-security/securing-your-devices/
- Ask for help if you need it:
  - IS&T Help Center: http://www.bu.edu/tech/about/help-center/
  - David Corbett, Medical Campus Information Security and BU HIPAA Security Officer, at corbettd@bu.edu

Once Device is OK, Keep it That Way

- 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

BOSTON UNIVERSITY

2. Data Storage Options

- BU network storage (RU-NAS/”HIPAA Drive”)
- Cloud:
  - BU Microsoft One Drive
  - BU’s Dropbox
- **Encrypted** Removable media (e.g., CD, DVD, USB key/stick)
- BU Google Drive-- for Confidential or Internal data only (not Restricted Use)

Check the BU IT site from time to time; IT is always looking for new secure options, and will add them here: http://www.bu.edu/tech/support/storage-options/

3. Data Sharing

Cloud sharing same as cloud storage:

- BU Dropbox
- BU Microsoft One Drive (Restricted Use) or
- BU Google Drive (Confidential)

Email: **Encrypt!**

1. Use Data Motion to send a secure **encrypted** email or
2. **Encrypt** the document or spreadsheet before attaching it.
   - *Tip:* Provide the password to the recipient by telephone - Do not send the password by email because it can be intercepted as well.

BOSTON UNIVERSITY

4. Foil Hackers and Fight Phishing!

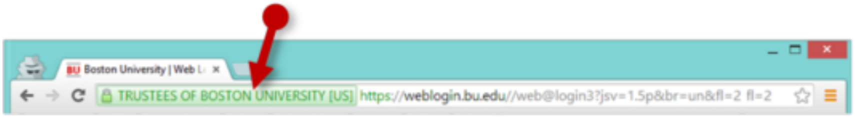
- Most people think it would never happen to them, but it regularly happens to BU faculty, staff, and students
- Typical signs:
  - Email asks for password – BU will never ask for login credentials through email
  - Appears to be from someone you know but has an unexpected attachment
  - Contains unexpected grammatical or spelling errors
- If there is any doubt, please forward the email to abuse@bu.edu and get advice

Learn more at BU's "How to Fight Phishing" webpage:
http://www.bu.edu/tech/services/cccs/email/unwanted-email/how-to-fight-phishing/

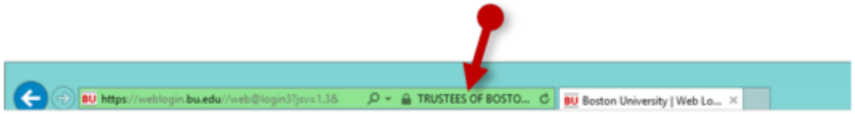
Check Before You Click

- 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

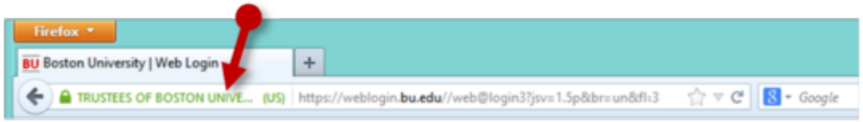
Chrome


BU 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


BU https://weblogin.bu.edu//web@login3?jsv=1.3&
TRUSTEES OF BOSTO...
BU Boston University | Web Lo... ×

Firefox


Firefox
BU Boston University | Web Login
+
TRUSTEES OF BOSTON UNIVE... (US) https://weblogin.bu.edu//web@login3?jsv=1.5p&br=un&fl=3
Google

Additional Tips: Safeguards for Working Remotely

Use the BU VPN (vpn.bu.edu)

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

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

Additional Tips: Protect Documents and Tangible Data

Do not remove documents or tangible data from the office.

If you do, 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.

BOSTON UNIVERSITY

BREACHES:
What are they?
How do I report?

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

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

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 your BU HIPAA Privacy and Security Officers, Information Security, OGC, and other BU offices. Your responsibility is to report any suspected security incidents to irt@bu.edu, and assist as requested in any investigation.

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:

- 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 forget the irt@bu.edu email address, report to the principal investigator, the IRB, or hipaa@bu.edu

BU prohibits retaliation for reporting security concerns, security incidents, and potential breaches

Additional Resources

- This PowerPoint will be available at www.bu.edu/hipaa
- BU Data Protection Standards: http://www.bu.edu/policies/information-security-home/data-protection-standards/
- BU HIPAA policies, forms and resources: http://www.bu.edu/hipaa
- 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