What You Need to Know About HIPAA and Data Security for Research

Diane Lindquist, JD*, Director Health Privacy and Compliance, BU*

David Corbett, JD, BBA*, Security Officer, BU Medical Campus*

Sean Nabi, JD, *Privacy Officer, Boston Medical Center*

Matt Ogrodnik, MS CIP*, Director, BUMC/BMC IRB.*

Overall objectives

- Present what is HIPAA, not HIPAA, and how it matters for research
- Describe what services investigators can use and which are not appropriate
- Understand when researchers should use BMC services or BU services
- Know how to secure devices and what resources are available
- Learn answers to common mistakes with HIPAA in the INSPIR application

Diane Lindquist, JD

Director Health Privacy and Compliance, BU

David Corbett, JD, BBA,

Security Officer, BU Medical Campus

HIPAA and
RESEARCH DATA SECURITY

For Boston Medical Center
and Boston University Medical Campus
Researchers

December 2018

BOSTON MEDICAL CENTER
EXCEPTIONAL CARE. WITHOUT EXCEPTION.

BOSTON UNIVERSITY

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

How does HIPAA impact researchers?

How to protect data - whether covered by HIPAA or not

How to report a possible breach of research data

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**: *health insurance plan* or *healthcare provider* that bills insurance companies

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

HIPAA and Research at BMC and BU

BU

- BU is a Hybrid Entity
- BU Covered Components: GSDM Dental Treatment Centers, BU Rehabilitation Services, Sargent Choice Nutrition Center, and the Danielsen Institute
- BU professional schools (BUSM, SPH) are not Covered Components. PHI disclosed to them for research purposes 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 almost anything else with patient or billing information, it is PHI subject to HIPAA

More Definitions

PHI: Protected Health Information, which means information about an individual's past, present, or future physical or mental health, and/or information about payment for, or provision of healthcare services, which is created or held by a Covered Component.

Business Associates: Persons or entities outside a Covered Component that perform a service for the Covered Component and need to create, receive, maintain, or transmit PHI to perform the service.

Business Associate Agreement: Obligates the Business Associate to keep our patient information secure. Must be in place before allowing Business Associate access to PHI, *even if the data is encrypted*.

18 Identifiers That Must Be Absent To Deidentify PHI

Most common ones needed in research bolded:

- ***Names***
- ***All geographic subdivisions smaller than a State (zip code)***
- ***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***

De-identification Alternatives

1. *Limited Data Set* (town/zipcode and dates ok)
   - Must enter into a Data Use Agreement

2. IRB approved HIPAA authorization or IRB Waiver (authorization not practicable)

3. Expert determination that there is a very small risk of identification despite having one or more of the 18 identifiers
   - Contact BU or BMC Privacy Officer

SAFEGUARDS

Biggest Risks:

Lost or Stolen

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

Cyberattack

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

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

Device Standards

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

- Operating system and applications are supported and updated
- Anti-Malware installed and set to auto update and scan
- Disk encryption
- Auto screen lock (15 min max) to password/code

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.

BU and BMC 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: send an email to bumchelp@bu.edu

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

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

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

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

BOSTON UNIVERSITY

Secure Resources

BU

Restricted Use:

- BU REDCap and MyCAP, Qualtrics, FreezerPro, WebCamp
- BU network Y Drive
- BU Microsoft SharePoint or OneDrive
- BU Dropbox (but not HIPAA data)

Confidential:

- All of the above, plus:
- Shared Computing Cluster (SCC 1-4)
- BU Google Drive

BMC

HIPAA Resources

- BMC network drive
- Box.com

Secure Email

BU Email

BU email does not have encryption – whenever you send RU data to (yyy@bu.edu)

- Use Data Motion to send a RU 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

Fight Phishing!

- Most people think it would never happen to them, but accounts are regularly compromised. **Red Flags:**
  - Email asks for password – BMC and 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 get advice:

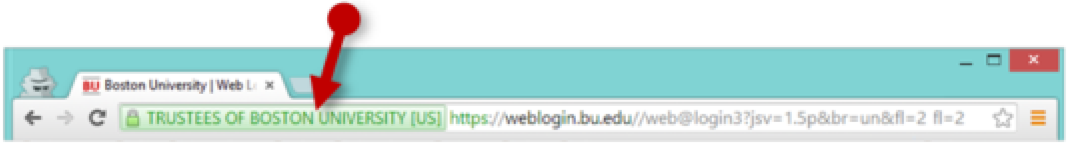
BU email: forward the email to abuse@bu.edu Learn more at our “How to Fight Phishing” webpage: http://www.bu.edu/tech/services/cccs/email/unwanted-email/how-to-fight-phishing/	**BMC email: forward suspect email to DG-Spam-attack@bmc.org**

Check Before You Click

Websites

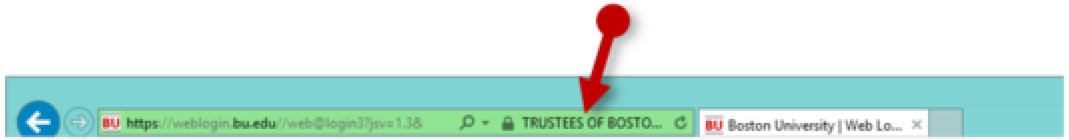
- Only enter login credentials if website address has **green** component and starts with https://
- Without the "s" preceding the colon, the website is not safe
  - Learn more at our "How to Fight Phishing" webpage

Chrome



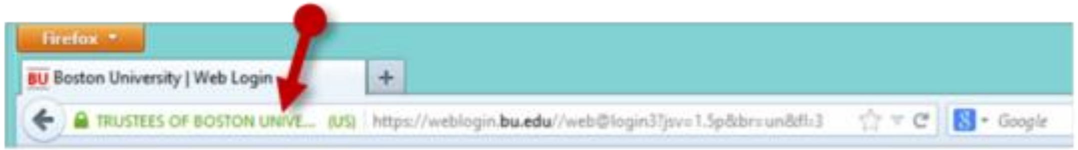
TRUSTEES OF BOSTON UNIVERSITY [US] https://weblogin.bu.edu//web@login3?jsv=1.5p&br=un&fl=2 fl=2

Internet Explorer



BU https://weblogin.bu.edu//web@login3?jsv=1.38 TRUSTEES OF BOSTO...

Firefox



TRUSTEES OF BOSTON UNIVE... (US) https://weblogin.bu.edu//web@login3?jsv=1.5p&br=un&fl=3

Safeguards For Working Remotely

Use BMC secure portal (https://mybmc.org or https://portal.bmc.org) or BU 2FA VPN (vpn.bu.edu/2fa)

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

Screen lock the device (Win + L)

Verbal Safeguards

- Do not discuss individuals outside closed offices

- Play music or background noise to disguise conversations

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

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?

What Events Must Be Reported?

Unusual system activity, including:

- Malware detections
- Unexpected logins
- 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

BU Resources:

- HIPAA Privacy Officer

Diane M. Lindquist

1 Silber Way Room 909

617-358-3124

dlindq@bu.edu

- HIPAA Security Officer

David C. Corbett

801 Mass. Ave,
Suite 485

(617) 358-0106

corbettd@bu.edu

Sean Nabi JD, CIPP/US

Privacy Officer for BMC

HIPAA and the IRB

MATTHEW OGRODNIK, MS, CIP
DIRECTOR INSTITUTIONAL REVIEW BOARD
BOSTON MEDICAL CENTER AND BOSTON UNIVERSITY MEDICAL CAMPUS

BOSTON MEDICAL CENTER
EXCEPTIONAL CARE. WITHOUT EXCEPTION.

BOSTON UNIVERSITY MEDICAL CAMPUS

HIPAA and the IRB

Learning Objectives

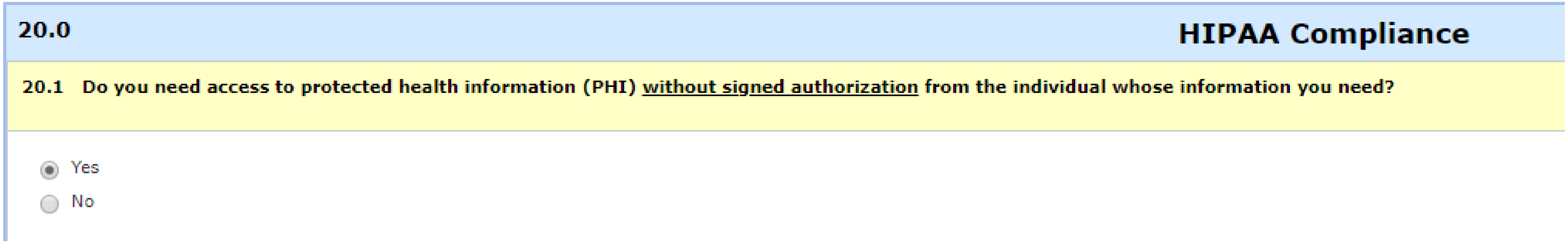
- Highlighting common mistakes with HIPAA in the INSPIR application
- Learn answers to submitted questions about HIPAA

HIPAA and the IRB

Learning Objectives

- Highlighting common mistakes with HIPAA in the INSPIR application
- Learn answers to submitted questions about HIPAA

HIPAA in INSPIR



20.0 HIPAA Compliance

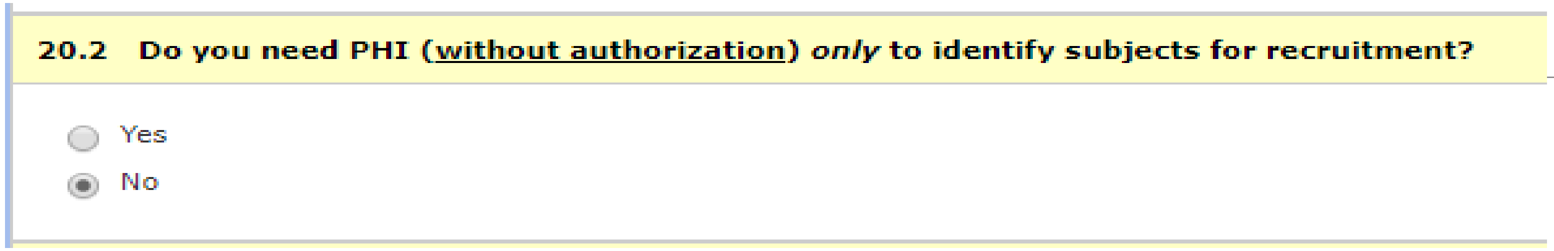
20.1 Do you need access to protected health information (PHI) without signed authorization from the individual whose information you need?

● Yes

○ No

- This question drives requesting a Waiver of HIPAA Authorization for research. This applies to both:
  - Use of PHI in situations where there is NO participant interaction
  - Use of PHI in situations where it is not possible to obtain a HIPAA signature
  - Or sometimes, both of these scenarios

HIPAA in INSPIR

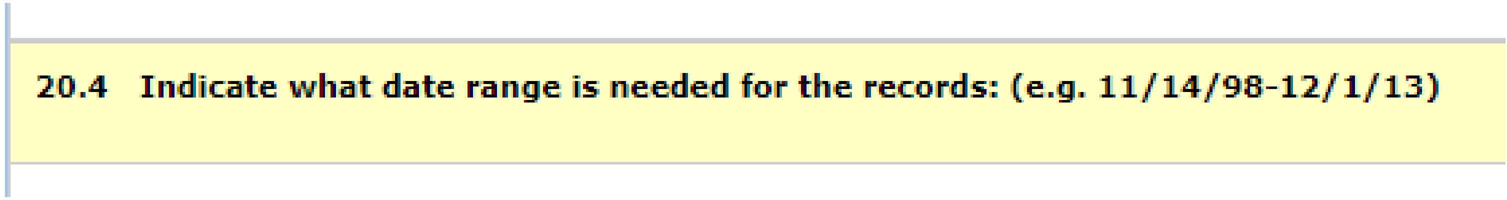


20.2 Do you need PHI (without authorization) *only* to identify subjects for recruitment?

○ Yes

● No

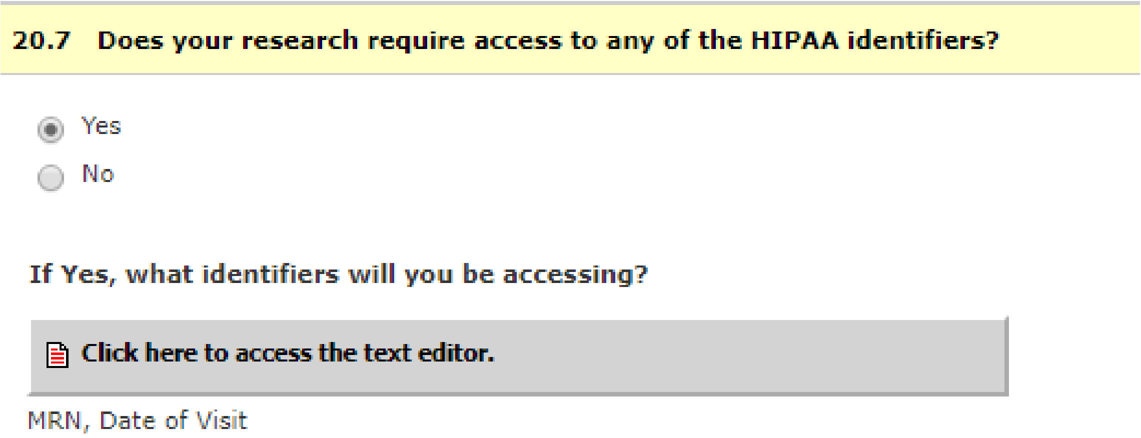
- Please answer Yes to this question if you are requesting a Waiver of HIPAA Authorization for recruitment ONLY
  - The classic scenario is medical/dental record pre-screening to identify patients who meet criteria



20.4 Indicate what date range is needed for the records: (e.g. 11/14/98-12/1/13)

- Please do not answer “1/1/2018 – Ongoing” as the IRB will not grant a waiver of authorization for indefinite use of PHI

HIPAA in INSPIR



20.7 Does your research require access to any of the HIPAA identifiers?

● Yes

○ No

If Yes, what identifiers will you be accessing?

MRN, Date of Visit

- The answer is always **Yes** if you (i.e. anyone from the study team) are accessing protected health information, even if you are not *recording* HIPAA identifiers in your dataset

HIPAA in INSPIR

To justify the waiver, you are asked to answer the following:

- Please describe why the research cannot be conducted without access to protected health information
- Why is it not practicable to obtain authorization from the participants?
- What is your plan to protect any identifiable information from use and disclosure by unauthorized parties?
- When and how will you destroy any identifiers linked to the data?

Please note that your answers to these questions should pertain ONLY to the data accessed/used via the Waiver; NOT to the data collected during the study once the participants have signed consent/HIPAA authorization

HIPAA and the IRB

Learning Objectives

- Highlighting common mistakes with HIPAA in the INSPIR application
- Learn answers to submitted questions about HIPAA

Questions about HIPAA

Q: Please review the HIPAA requirements when doing research using EMR data.

A: A Waiver of authorization is needed if the study team is accessing PHI that goes beyond a Limited Data Set. For example – if the study team is directly abstracting data from the EMR, a Waiver must be requested because you need to access name, MRN, etc, to be in the patient chart.

Questions about HIPAA

Continued…

Q: Please review the HIPAA requirements when doing research using EMR data.

A: If, however, the CDW is providing all data either fully de-identified or as a Limited Data Set, a Waiver is not needed. This does not really affect the INSPIR user, however; the HIPAA section in INSPIR remains the same, as the IRB makes the HIPAA determination for you.

Questions about HIPAA

Q: What should be done if you go past the HIPAA waiver of authorization timeframe?

A: Please submit an amendment to request an extension of the date range that is needed for the records. The amendment request should provide a justification as to why this is needed.

Questions about HIPAA

Q: What are the HIPAA requirements for qualitative studies done at BU?

A: If the study PI is a BU investigator, HIPAA only applies if you are accessing BMC medical records – either for recruitment, for example, or to supplement the qualitative data. If all data comes directly from the participant (in an interview or survey, for example), HIPAA does not apply.

Questions about HIPAA

What questions do you have?

Questions and discussion

Thank you!!