



BOSTON UNIVERSITY MEDICAL  
CAMPUS

# CRRO Privacy and Data Security

Presented by Erika Barber, BMC Director of Compliance and Privacy  
David Corbett, BUMC InfoSec Officer  
Scott Pasquino, BMC Hospital InfoSec Officer

# Learning Objectives

---

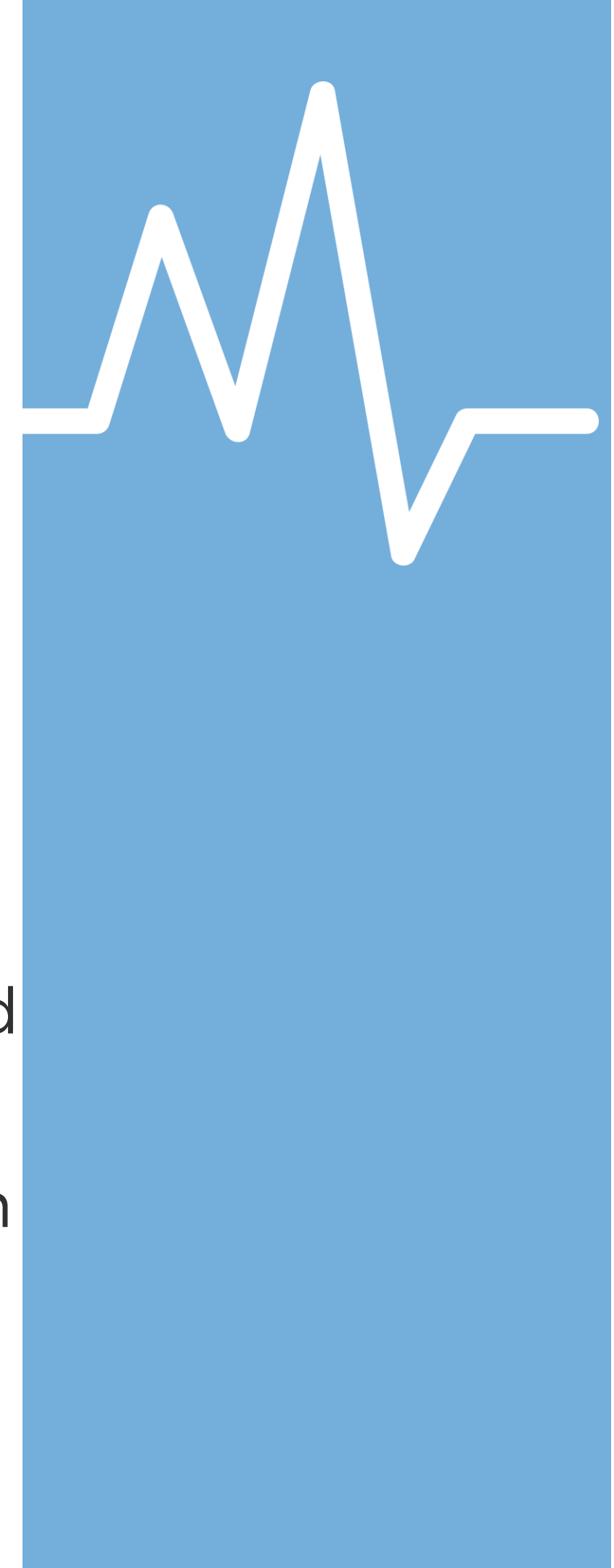
## Important Points to Discuss

- Privacy Basics
- Security Basics
- How to Report a Security Incident or Breach

# Data Use or Transfer Agreements

---

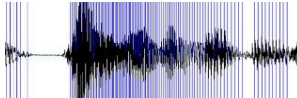
- When is a Data Transfer Agreement (“DTA”) required?
  - When receiving or transferring data with a third party (including between BU and BMC)
- When is a Data Use Agreement (“DUA”) required?
  - When sharing or receiving a *limited data set*, as defined by HIPAA
  - This is a regulatory requirement under HIPAA in certain instances

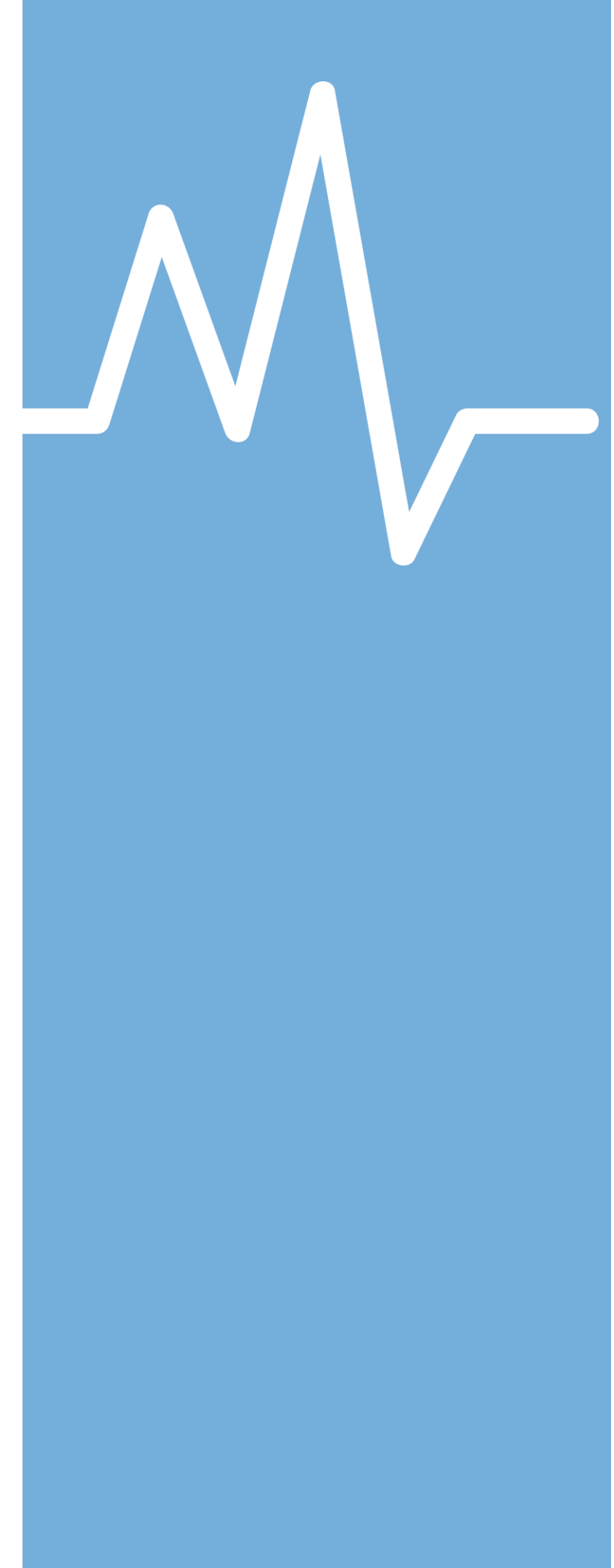


# Data Transfers - HIPAA Identifiers

There are 18 HIPAA identifiers.

Having **just ONE** of the 18 data variables can render a data set fully identifiable or a limited data set

- Name
- Address (all geographic subdivisions smaller than state, including street address, city county, and zip code)
- All elements (except years) of dates related to an individual (including birthdate, admission date, discharge date, date of death, and exact age if over 89)
- Telephone numbers
- Fax number
- Email address
- Social Security Number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate or license number
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web URL
- Internet Protocol (IP) Address
- Finger or voice print 
- Photographic image - Photographic images are not limited to images of the face.
- Any other characteristic that could uniquely identify the individual



# Data Transfers

- Classify the data set under HIPAA

## Fully Identified

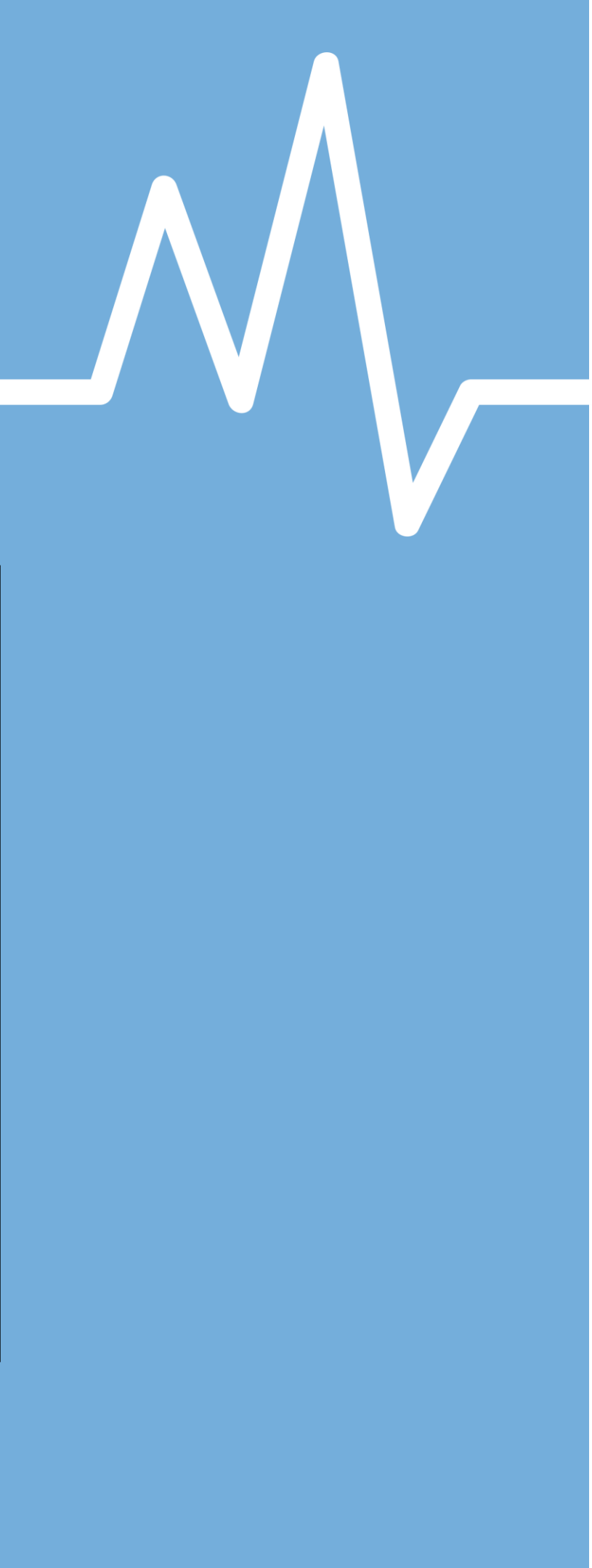
- Certain identifiers (e.g., name)
  - May be shared pursuant to *(1) HIPAA authorization or (2) IRB waiver, and data transfer agreement / DTA*

## Limited Data Set

- Does not contain 16 of the identifiers, but CAN include:
- Dates such as admission, discharge, service, DOB, DOD; and
- City, state, zip code.
  - May be shared pursuant to a *data use agreement / DUA*

## Fully DE-identified:

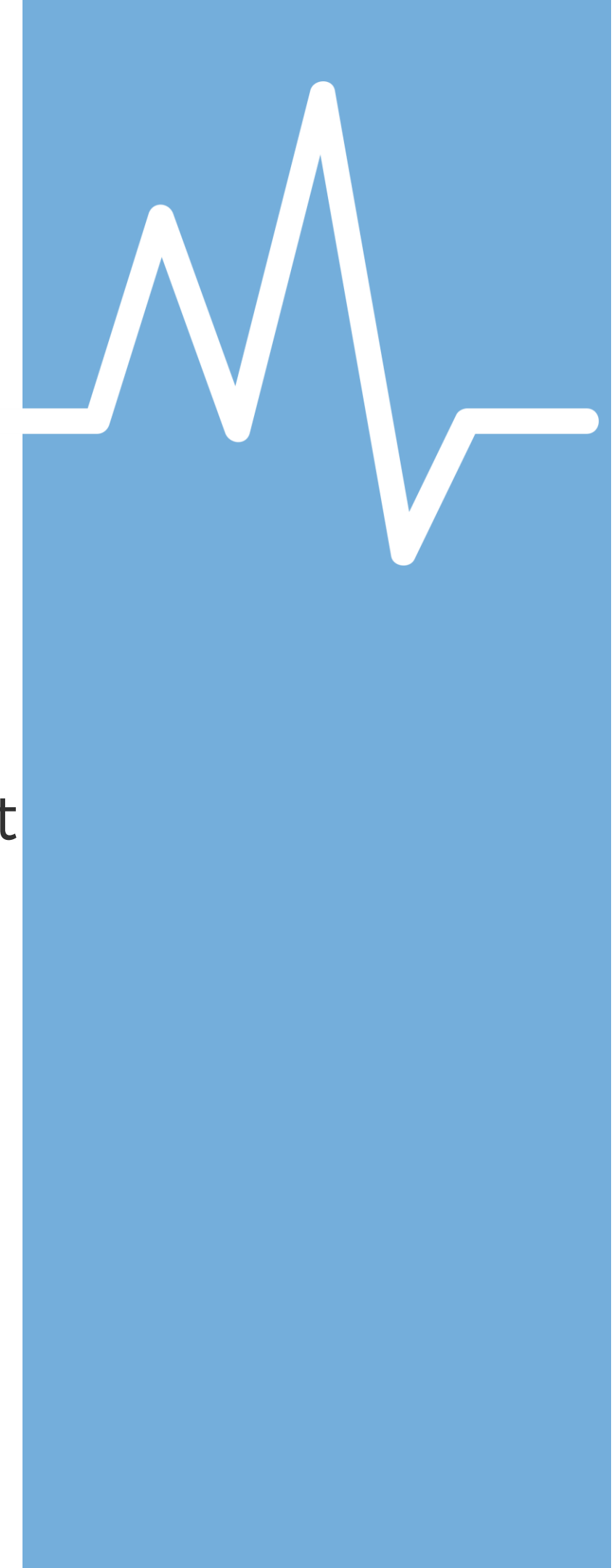
- NONE of the 18 identifiers
  - May be shared pursuant to *data transfer agreement / DTA*



# Data Transfer of PHI - Three Pathways to Success

---

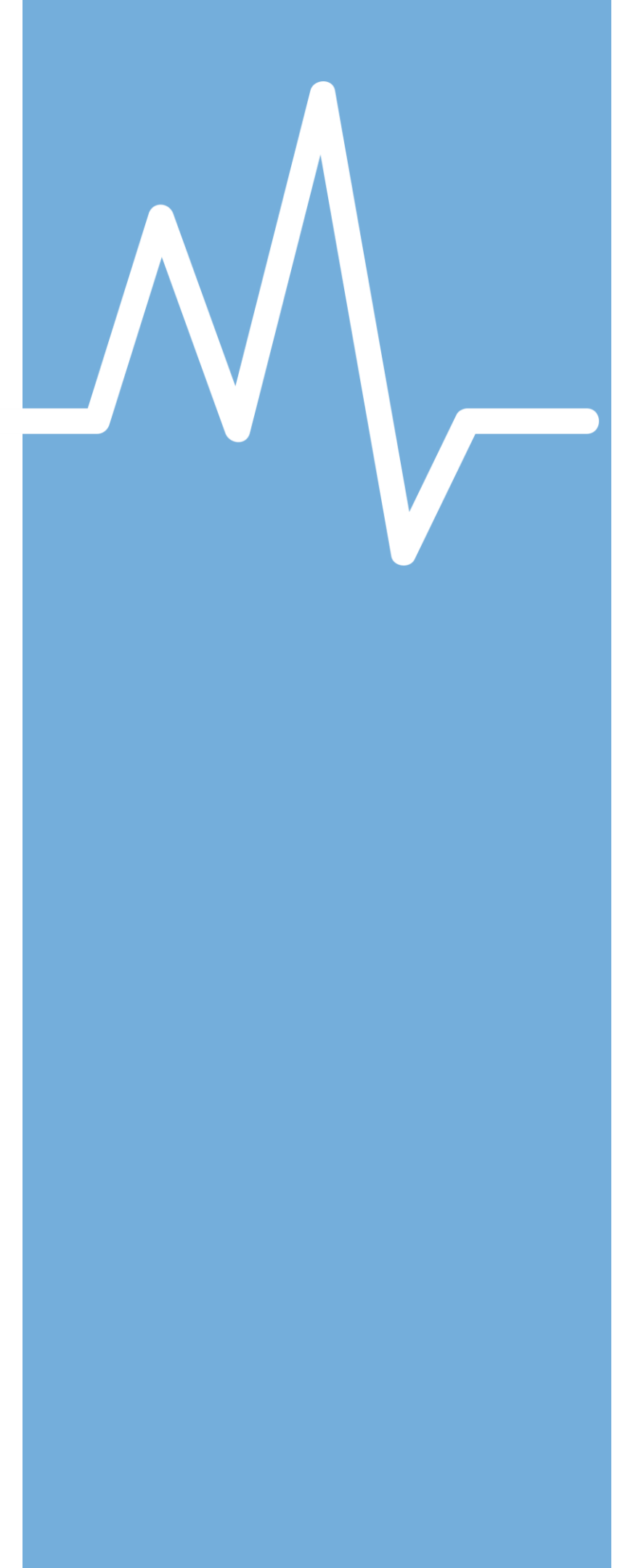
- HIPAA has certain requirements for data transfers
- In the research context, the main three ways to properly transfer protected health information are:
  - Via a **HIPAA authorization** (typically as part of a consent form) contemplating such disclosure
  - Via an IRB-approved *waiver* of HIPAA authorization
  - Via a **data use agreement** for a *limited data set*



# Data Transfer Agreement Requests

---

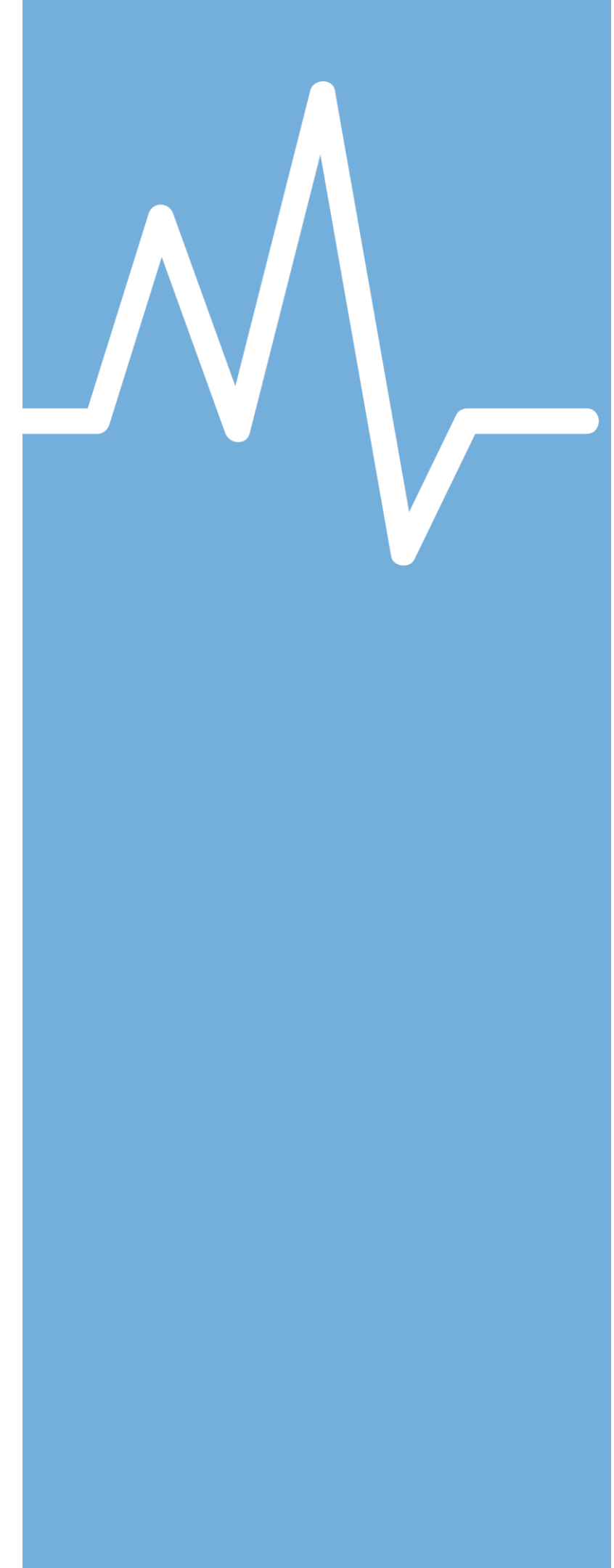
- Request an Agreement
  - BU Office of Sponsored Programs
  - BMC Grants & Contracts Office
  - Links to forms at end of training



# Personal Cell Phone Use

---

- Personal cell phone use
  - BMC (AirWatch)
- Searching subject address and contact information?
  - Google search is acceptable
  - But deeper search tools, like Spokeo, are discouraged because they can provide additional data
- Phone call best practices
  - Setting or location
  - Don't leave detailed messages

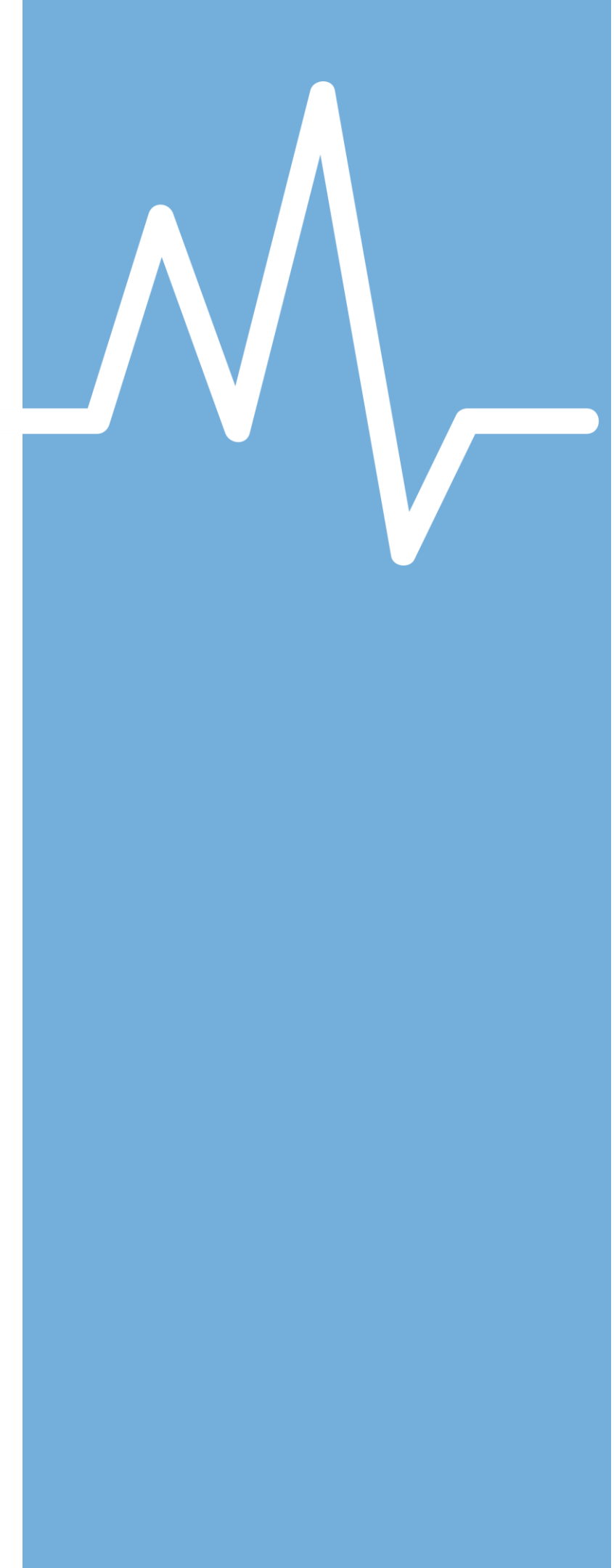




# Texting

---

- Texting needs to be approved by the IRB
  - Anything with subject data
  - Must mention security risk of texting in Informed Consent
- BMC Medumo
- BU REDCap and Twilio



# Zoom Best Practices

---

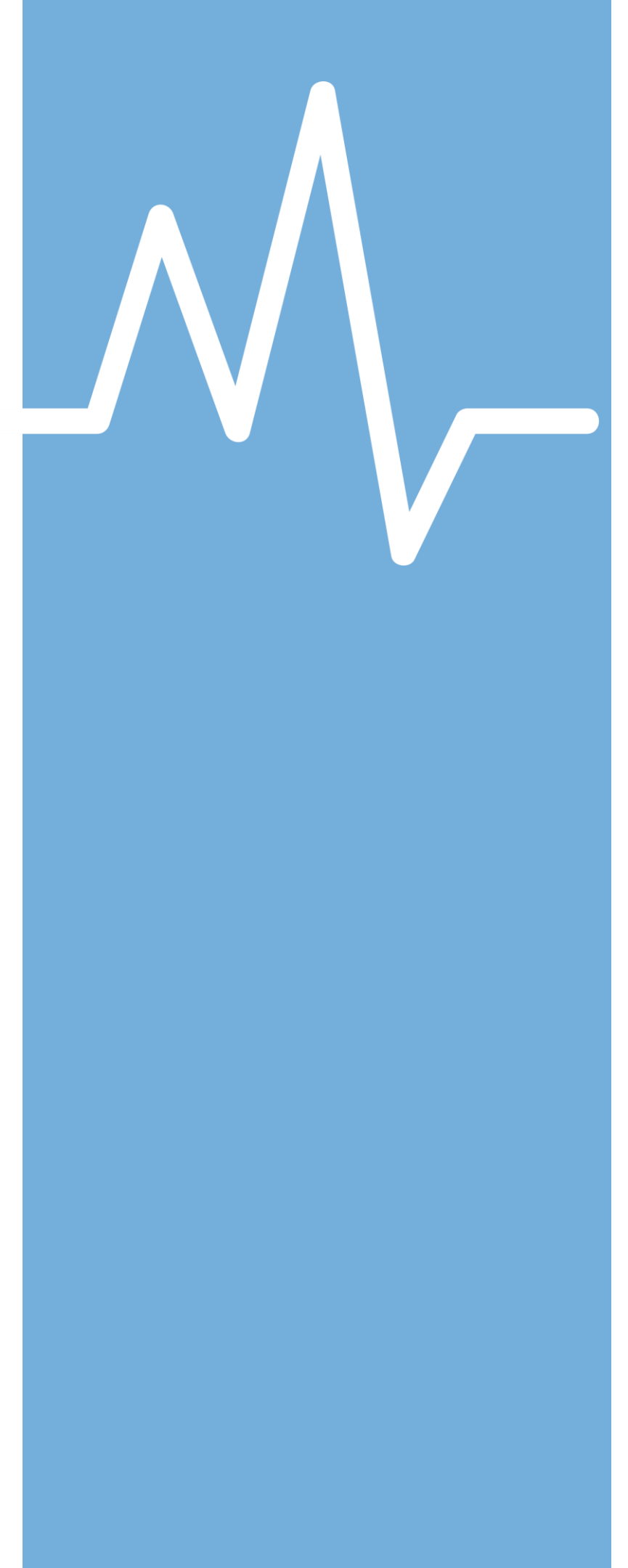
- At BU there are two types of Accounts
  - Regular Zoom
  - Zoom meetings for HIPAA (BMC)
- Best Practices
- Get verbal consent for
  - group meetings to ensure they are aware they are a part of group treatment
  - Any recordings



# Data Retention

---

- Sponsored research records need to be kept for 7 years minimum (research sponsor could require longer)
- Secure BMC or BU storage
- Going to another institution?
  - Data Transfer Agreement



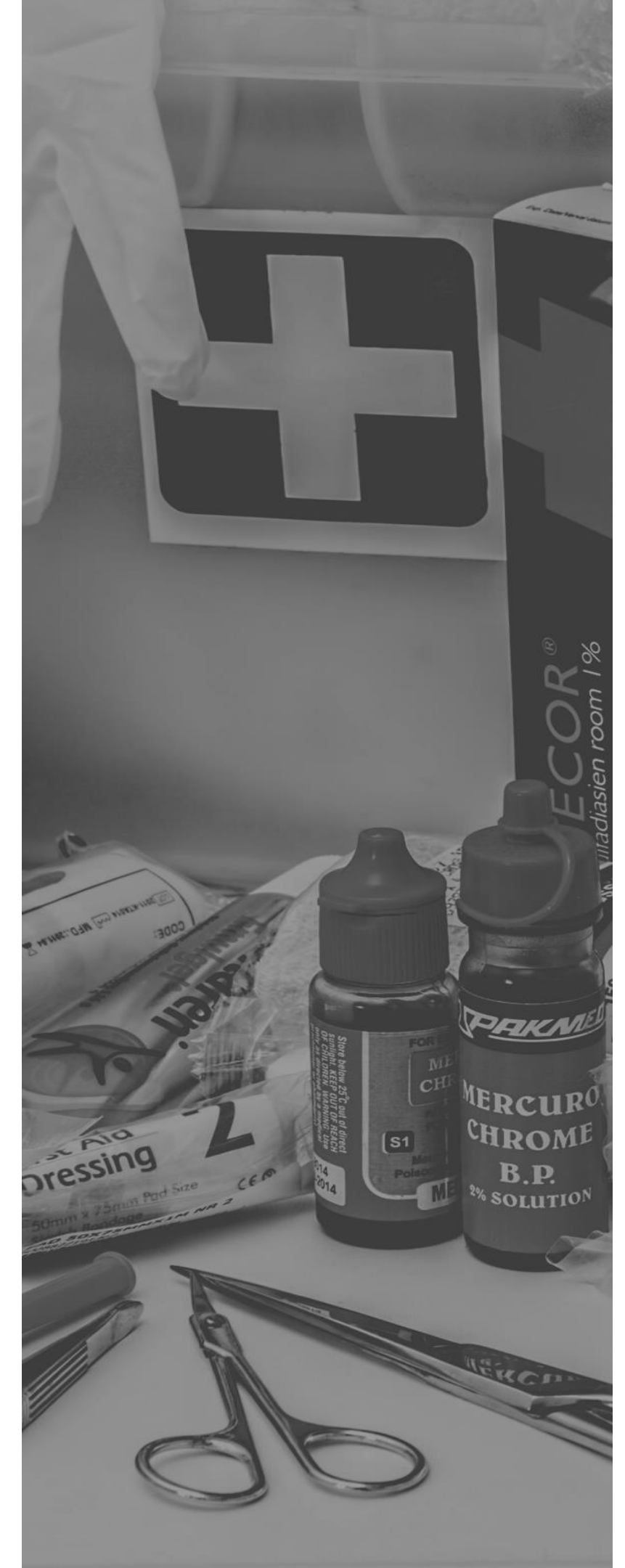
# What's The Big Deal?

---

## Feinstein Institute for Medical Research

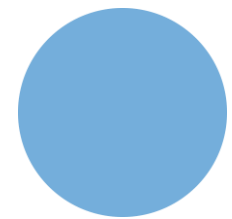
An unencrypted laptop was stolen from a car, containing data of about 50 research studies and approximately 13,000 individuals

- **Big money payment:** settled alleged HIPAA violations for \$3.9 million
- **Ongoing government scrutiny:** three year corrective action plan
- **Loss of confidence and reputation**

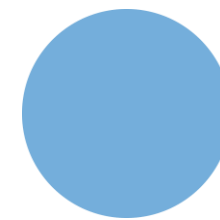


# SECURE YOUR DEVICES

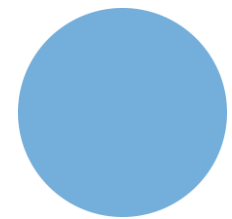
**Every device (e.g., desktop, laptop, tablet) used to access, process, or store patient or research data must have:**



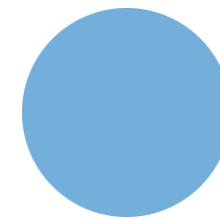
Operating system that is supported and updated



Auto screen lock (15 min max)

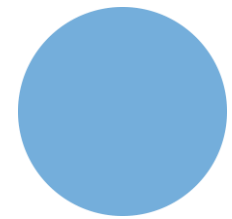


Anti-malware (CrowdStrike free)

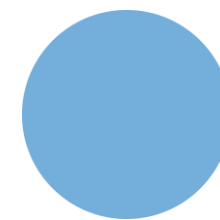


Disk encryption

**Phones are made secure by:**



Requiring a pin/code or biometric automatically turns on encryption



Disabling cloud sync for any HIPAA data

# BU Data Protection Standards, Classification Policy

## **Restricted Use (BMC Confidential)**

Loss or misuse may require notification to individuals or state/federal government, includes:

- HIPAA, individually identifiable health information used in research
- SSN, driver license #, debit/credit card #, checking account # (billing records)

## **Confidential**

Loss or misuse may adversely affect individuals or BU business, includes:

- FERPA
- Anonymized data or HIPAA Limited Data Set: dates, city, zip code

## **Internal**

Potentially sensitive, requires protection from disclosure

## **Public**

Does not require protection from disclosure



# Collecting, Storing, & Processing

## BU Restricted Use - BMC Confidential

- BU REDCap / MyCap
- BU Qualtrics
- BU Zoom or Teams for communication
- BU O365 SharePoint, OneDrive, PowerBI, Stream
- BU RU-GPNAS (BUMC Network Y Drive)
- BMC network drive or BMC Box.com
- Full list of reviewed services is on the BUMC IT website

## Confidential

- Above plus MGHPCC Shared Computing Cluster (SCC4)

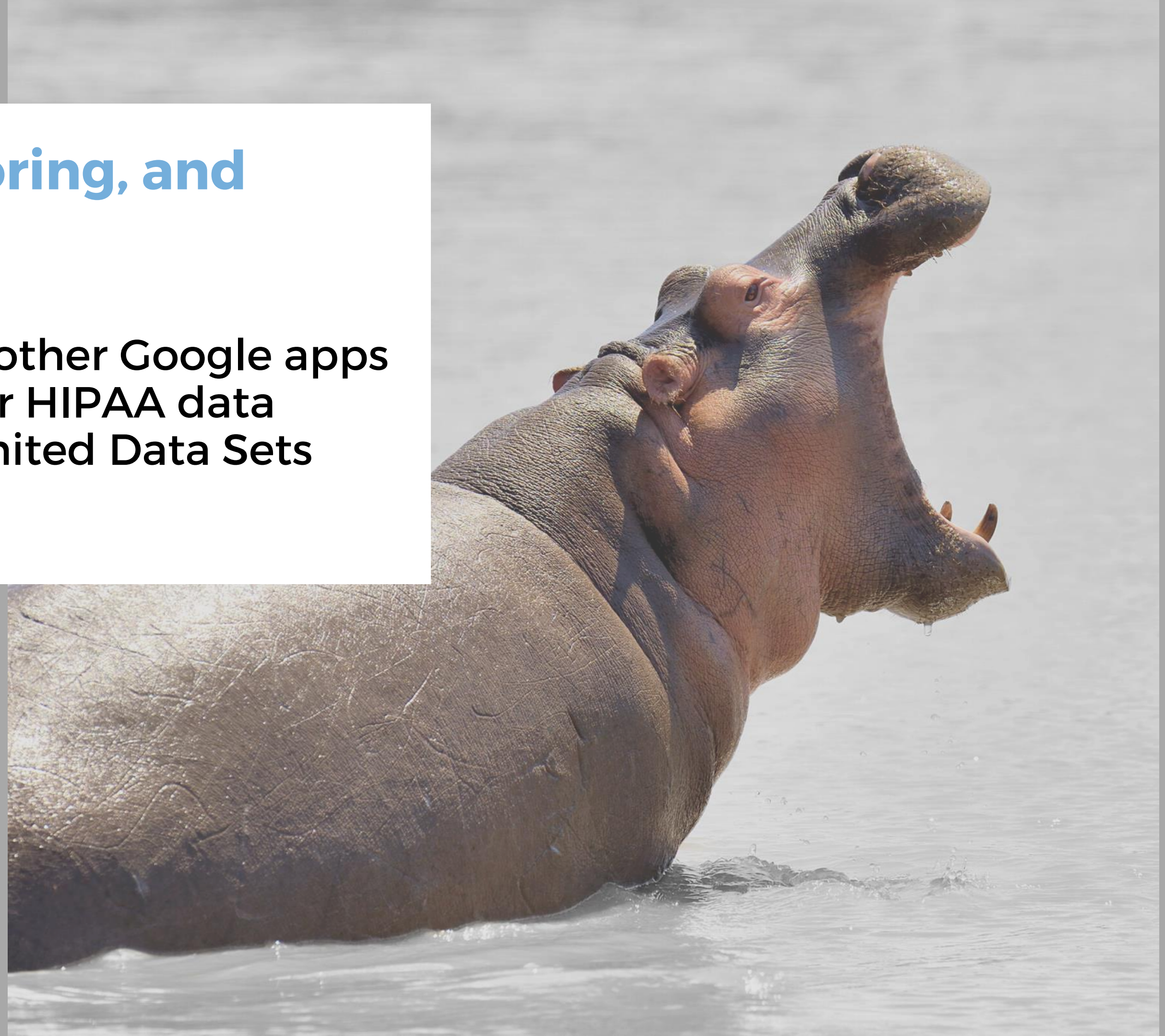




# Collecting, Storing, and Processing

---

Google Drive and other Google apps cannot be used for HIPAA data or even HIPAA Limited Data Sets





# Medical Device Best Practices

## IRB Application

- Include in IRB application
- Mention any security concerns in Informed Consent form

## Best Practices

- HIPAA research cannot use Apple Cloud
- USB transfer presents lower risk
- If wireless transfer, consider anonymization (subject ID)



# Email

## BMC Email

- Type “secure” in the subject line
  - User will receive a receipt with a link to access the secure mail

## BU Email options

Outlook and Gmail cannot be used – no encryption

- Use Data Motion to send a secure email or
- Encrypt the document or spreadsheet before attaching it.
  - Don't identify patients in the body or subject of the email
  - Don't send passwords for attached encrypted files by email

## File Sharing alternatives

- BMC Box.com
- BU Office365 SharePoint or OneDrive
  - Share site, folder, or file



# PHISHING

Phishing is one of the easiest forms of cyber-attack for a criminal to carry out and one of the most widespread. By responding to or clicking on a phishing email you risk:

- Downloading harmful malware, spyware & viruses
- Handing over your login credentials, your login and password

Think before you Click! Look for the following warning signs with any email you receive to avoid being phished:

- **Requests for Personal Info:** (BMC/BU will never ask you for your password)
- **Poor Grammar:** Odd wording, misspellings and errors
- **Urgency:** Calls to take immediate action or threats of consequence
- **Sender:** Check the sender's email  
[username.bu.edu@outlook.com](mailto:username.bu.edu@outlook.com)  
[username.bu.edu@gmail.com](mailto:username.bu.edu@gmail.com)  
[username.bu.edu@my.com](mailto:username.bu.edu@my.com)
- **Links & Attachments:** Stop! Verify a file before downloading and hover over links

**Suspicious email? Forward to [abuse@bu.edu](mailto:abuse@bu.edu) or [spam@bmc.org](mailto:spam@bmc.org)**



# WHAT IS A BREACH?

A breach is any unauthorized access, use, or disclosure of patient information (includes unintentional)

- Theft or loss of devices
- Unauthorized viewing/accessing, including snooping
- Handing or sending data to wrong person
- Hacking / Cyberattack

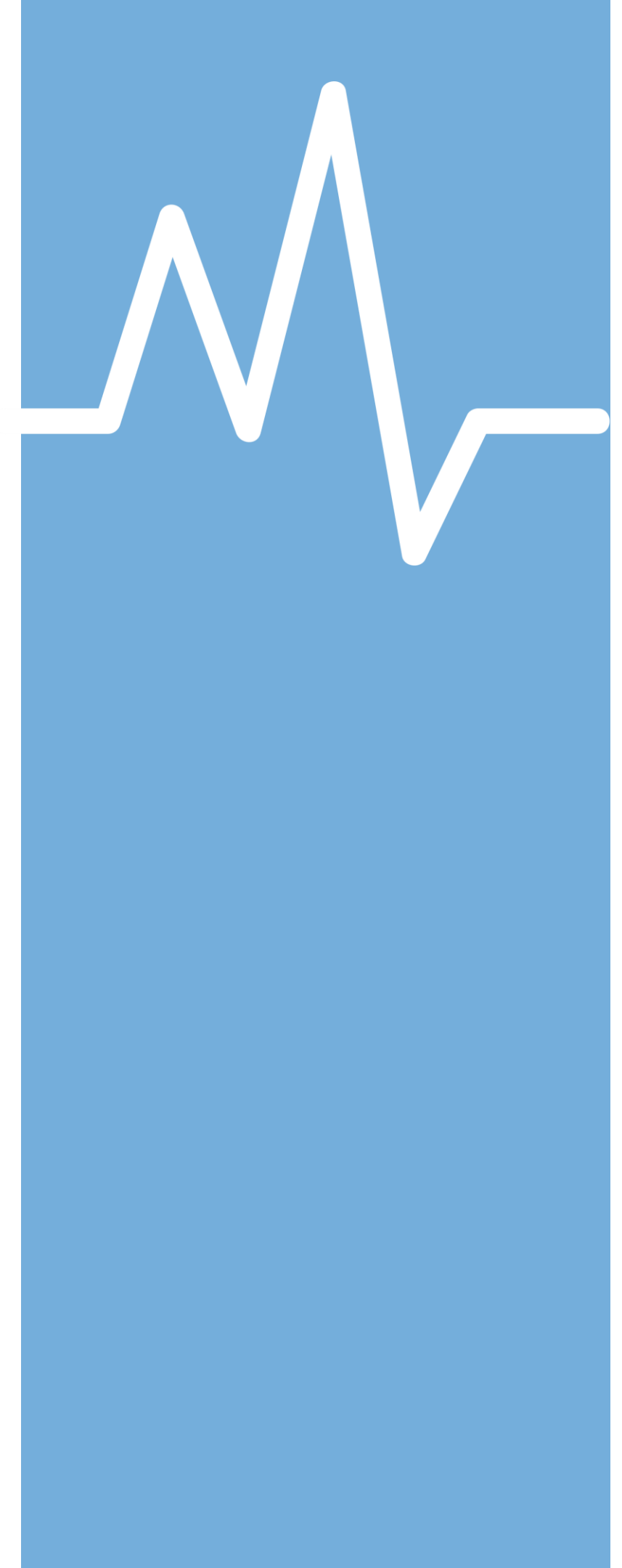


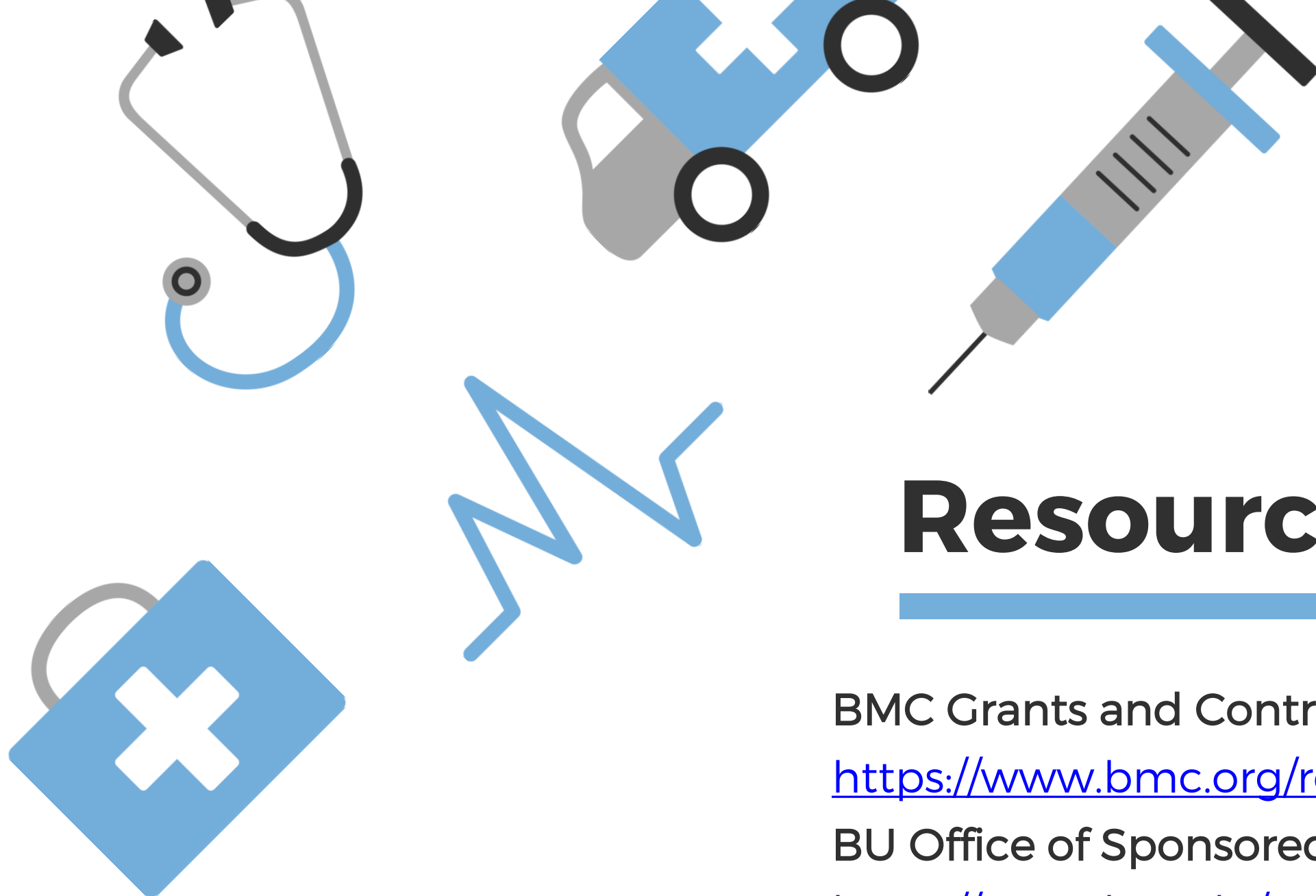
# Reporting a Security Incident or Breach

---

- BU Incident Response Team ([irt@bu.edu](mailto:irt@bu.edu))
- BMC Privacy Officer ([privacyofficer@bmc.org](mailto:privacyofficer@bmc.org))
- IRB Reportable Events and New Information (RENI)
- BMC or BU will determine what steps are required, such as reporting
- Any reporting to NIH or Sponsor will come after internal reporting

**We'll assess the situation, determine whether any notifications need to be made, and help you analyze how similar events can be prevented**





# Resources

---

BMC Grants and Contracts Office

<https://www.bmc.org/research-operations/forms>

BU Office of Sponsored Programs

<https://www.bu.edu/researchsupport/>

Securing Devices: <https://www.bumc.bu.edu/it/infosec/>

Approved apps: <https://www.bumc.bu.edu/it/infosec/researchcompliance>

BMC Privacy

[privacyofficer@bmc.org](mailto:privacyofficer@bmc.org)

BUMC Information Security

[bumcinfosec@bu.edu](mailto:bumcinfosec@bu.edu)

BMC Hospital Information Security

[scott.pasquino@bmc.org](mailto:scott.pasquino@bmc.org)

# Questions

---

