Where is the Data?
Risks of Data Location, Storage
and Protection of Sensitive
Protected Health Information

Holly Benton, JD, CHPC
Associate Compliance Officer, Privacy

Margaret Groves, JD, CFA, CHPC, CHRC
Associate Compliance Officer, Human Subject Research Compliance

Session Objectives

• Identify how to capture your institution’s information asset landscape and identify sensitive data and PHI.
• Discuss research data security and storage plans as an effective method for monitoring sensitive information, regardless of form, across the institution.
• Highlight considerations regarding data transfers between institutions when faculty arrive and leave.
• Get tips for safeguarding your institution.

Now, a little about you...
Knowing where your sensitive data is takes a few steps...

1st Step: IDENTIFY YOUR INFORMATION ASSET LANDSCAPE

Um, excuse me, do what?!
How!?! (cont’d.)

Survey and Inventory
A Privacy Impact Assessment, or PIA, is an analysis of how sensitive information is collected, used, shared and maintained at your institution.

A PIA identifies:

**Who**
- Who is collecting sensitive information

**What**
- What is collected

**Why**
- Why it is collected

**How**
- How it is collected, used, accessed, shared, safeguarded and stored
A PIA is a decision tool to identify and mitigate institutional privacy risk:

- Ensure legal, regulatory and institutional policy compliance.
- Determine associated risks and effects.
- Evaluate protections and alternative processes to mitigate potential privacy risks.

Does your organization currently conduct PIAs or otherwise inventory sensitive data?

Tips
- Identify institutional partners
- Conduct PIAs
  - Survey the institution for sensitive information
  - Inventory sensitive data and related information asset management practices
  - Risk assess information management
- Identify gaps against compliance requirements
- Engage institutional partners to address gaps
- And...
2nd Step: MAINTAIN ONGOING CONTROL

Annual Update Model
- Provides information if data has moved or system has changes
- Can be tied to IRB renewal
- Is research unit- or other owner-driven
- Serves as a central repository for annual update information
- Management takes responsibility for knowing where data resides!

Duke’s Research Data Storage Plans (RDSP)
- Tied to submitted protocols
- Specify storage location
- Identify classification of data being collected
- Reviewed by IT personnel
- Research unit sign-off
- Included in eIRB with study protocol information
- Study team responsible for plan accuracy

Annual Update Model
- Provides information if data has moved or system has changes
- Can be tied to IRB renewal
- Is research unit- or other owner-driven
- Serves as a central repository for annual update information
- Management takes responsibility for knowing where data resides!

Duke’s Research Data Storage Plans (RDSP)
- Tied to submitted protocols
- Specify storage location
- Identify classification of data being collected
- Reviewed by IT personnel
- Research unit sign-off
- Included in eIRB with study protocol information
- Study team responsible for plan accuracy
Other Protection Tools:

• Data Loss Prevention®
  – January 2013
  – The Data Loss Prevention program: Software that allows for the protection of sensitive and confidential information on the Duke Health Network.
  – Monitors sensitive information, such as PHI and financial information, that leaves the institution.
    • Email encryption.
    • No sensitive information in the subject line.

• FairWarning®
  – Privacy surveillance tool Compliance employs to systematically audit and review EHR and billing access.
  – Assists with identifying unauthorized faculty and staff access of household members’, VIP’s and others’ records.
  – Patient authorization: Staff may download the Authorization to Protected Health Information Form from HIM webpage or may request the form from HIM. MUST be completed and signed by the patient / patient representative and forwarded to HIM.

Does your institution have something similar to an RDSP?
Does your institution have other data loss prevention mechanisms?

3rd Step: COMMUNICATE AND MONITOR

Communication is the key to effective compliance.
Ensure everyone gets the message!

To get to all, it takes different paths...

The ‘To Do’ List:
- Define responsibilities and requirements
- Message via multiple platforms
- Provide accessible resources and SMEs
- Emphasize a culture of compliance
- Provide ongoing, updated training
How do you communicate?

And to mitigate risk and protect the institution...

monitor.

Activities to Monitor

- Collection and use of PHI without subject authorization and/or a HIPAA waiver.
- Storing research data, especially ePHI, on unencrypted computers and/or portable devices.
- Storing research data in non-institutionally approved and/or managed locations.
Activities to Monitor (cont’d.)

- Retention of Social Security numbers in subject files without an authorized exception.
- Missing ICFs, source documents or other documents containing PHI.
- Failing to adhere to the minimum necessary standard.
- Improper disposal and/or destruction of PHI.

Activities to Monitor (cont’d)

- Disclosing PHI without the appropriate agreements executed and/or without authorization.
- Unencrypted transmission of PHI and/or other sensitive electronic information.
- Use of unapproved, unmanaged copy or fax machines.
- Use of personal email (Gmail, Yahoo, etc.) for institutional business.

To Secure Protected Health Information...

... Encryption is the key!

Protect It
- Store or sync files containing PHI.
- Only use Duke's shared network or Duke Box secure cloud storage.

Encrypt It
- All portable devices storing PHI should be configured for encryption: thumb drives, USB hard drives, cell phones, tablets.

Sync It
- All smartphones & tablets accessing PHI must sync with Duke's Exchange email service to ensure encryption.

For information on securely configuring mobile devices:
- Visit: security.duke.edu/secure-your-devices/mobile-devices
Faculty Arrival

Things to consider:
- What are individuals bringing with them?
  - Data (Did subjects consent to transfer of identifiable data?)
  - Samples (level of identification)
  - Equipment (what data may still reside on equipment from another institution)
- Where are they coming from?
  - Domestic
  - International

Faculty Departure

Things to consider:
- Ongoing status on the project(s)
- Level of future involvement
- What do they want to take with them?
  - Samples / data / equipment
- Where are they going?
  - Domestic / international
Questions?

Our Contact Information:

Holly Benton, JD, CHPC
Associate Compliance Officer, Privacy
holly.benton@duke.edu

Margaret Groves, JD, CRA, CCRP, CHRC
Associate Compliance Officer, Human Subject Research Compliance
margaret.groves@duke.edu
Sources

- Images used in this presentation that are not in the public domain are used per the terms of their Creative Commons copyright licenses:
  - "Background Stairs," by Julie Gentry [CC0]; "Boy (Anders) with Binoculars," Jrod2 commons.wikimedia.org [CC BY-SA]; photo of baby, okc-craigslist.blogspot.com [CC BY-ND]; "Ralls Texas Grain Silos 2010," by Leaflet, commons.wikimedia.org [CC BY-SA]; Survey graphic, 10EnglishCM.wikispaces.com [CCO]; Gold key, openclipart.com [CC0]; Brizzle born and bred, free-photos.gatag.net [CC BY-ND]; photo of paths, decoracaoacoracao.blog.br [CC0]; Silent film director D.W. Griffith using megaphone in 1922, unknown photographer [CC0]; hands holding house image, by Geralt, pixabay.com [CC0].

- Flow charts adapted from the Duke Department of Community and Family Medicine Faculty Arrival and Departure Flowchart https://oarc.duke.edu/sites/default/files/documents/Faculty%20Arrival%20and%20Departure%20Flowsheet%20404216.pdf