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, CRA, CHRC, CHRC
Associate Compliance Officer, Human Subject Research Compliance

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

1

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.

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

2

Now, a little about us you…

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

3

Knowing where your sensitive data is takes a few steps…

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

4

1st Step: IDENTIFY YOUR INFORMATION ASSET LANDSCAPE

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

5

Um, excuse me, do what?!

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

6

How!?!

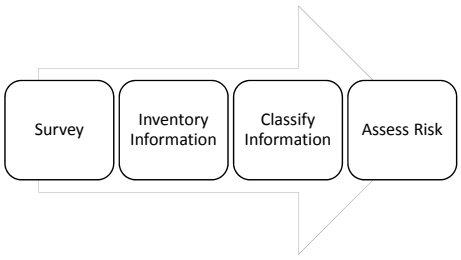
Duke | OFFICE of AUDIT, RISK & COMPLIANCE 7

How!?! (cont'd.)

Duke | OFFICE of AUDIT, RISK & COMPLIANCE 8

Survey and Inventory

Duke | OFFICE of AUDIT, RISK & COMPLIANCE 9



Duke | OFFICE of AUDIT, RISK & COMPLIANCE

10

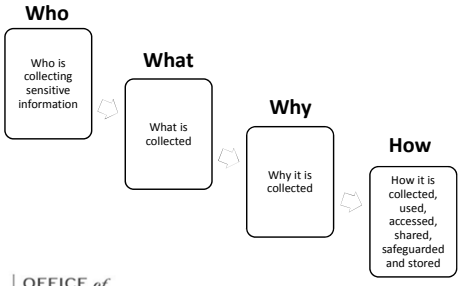
Conduct a Privacy Impact Assessment

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

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

11

A PIA identifies:



Duke | OFFICE of AUDIT, RISK & COMPLIANCE

12

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.

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

13

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

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

14

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….

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

15

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

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.

Duke | OFFICE of AUDIT, RISK & COMPLIANCE 19

Other Protection Tools:

- 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', VIPs' 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.

Duke | OFFICE of AUDIT, RISK & COMPLIANCE 20

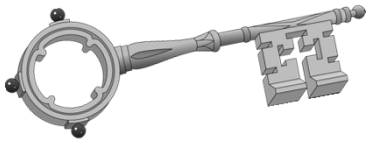
Does your institution have something similar to an RDSP?

Duke | OFFICE of AUDIT, RISK & COMPLIANCE 21

Does your institution have other data loss prevention mechanisms?

3rd Step: COMMUNICATE AND MONITOR

Communication is the



to effective compliance

Ensure everyone gets the message!

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

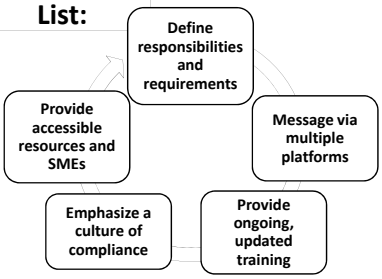
25

To get to all, it takes different paths…

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

26

The 'To Do' List:



Duke | OFFICE of AUDIT, RISK & COMPLIANCE

27

How do you communicate?

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

28

And to mitigate risk and protect the institution…

monitor.

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

29

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.

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

30

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.

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

31

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.

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

32

33

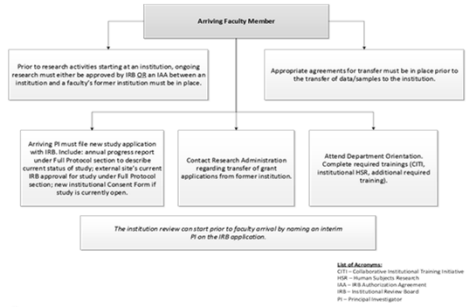
Faculty Arrival

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

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

34



Duke | OFFICE of AUDIT, RISK & COMPLIANCE

35

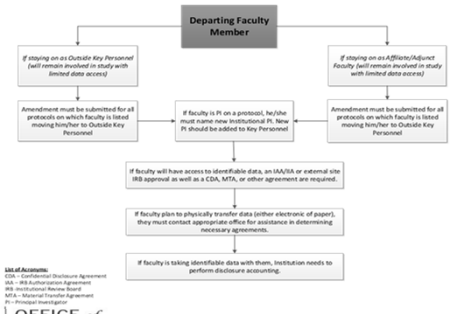
Faculty Departure

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

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

36



Duke | OFFICE of AUDIT, RISK & COMPLIANCE

37

Questions?

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

38

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

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

39

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-commonswiki, CC BY-SA; photo of baby, okc-craigslist.blogspot.com, CC BY-ND; photo of ocean, oneirokriths123.com, CC BY; "Ralls Texas Grain Silos 2010," by Leaflet, CC BY-SA; Survey graphic, 10EnglishCM.wikispaces.com, CCO; Gold key, by Firkin, openclipart.com, CCO; 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, CCO; 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 Flowsheet https://oarc.duke.edu/sites/default/files/documents/Faculty%20Arrival%20and%20Departure%20Flowchart%20042216.pdf

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

40