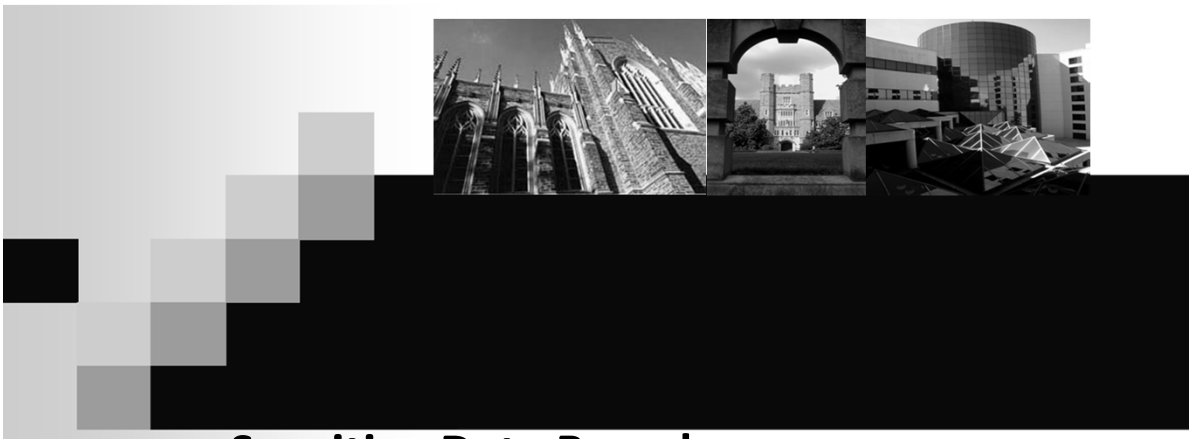


Sensitive Data Breach: Not If, But When

June 5, 2017

Holly Benton, JD, CHPC
Associate Compliance Officer, Privacy

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

1

Session Objectives

- Discuss why it's "Not if, but when" when it comes to a data breach in higher education.
- Highlight the risk mitigation value of knowing what sensitive institutional information assets you have, where they are and why you need to know.
- Offer methods of identifying and monitoring sensitive information, including leveraging partners and using tools such as PIAs and RDSPs.
- Provide an example of managing information flow: onboarding and departing faculty.

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

2

But first, about me you…

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

3

What exactly does "Not if, but when," mean?

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

4

Breach: Not If, When…
No Industry Immune

Category	# of Breaches	% of Breaches	# of Records	% of Records
Bank/Cred/Fin	18	3.5%	20,000	0.2%
Business	285	55.2%	7,494,791	80.6%
Educational	68	13.2%	41,448	0.4%
Gov/Military	27	5.2%	188,933	2.0%
Med/Healthcare	118	22.9%	1,548,027	16.7%
TOTALS	**516**	100.0%	**9,293,199**	100.0%

- As of April 26th 2017, Data Breach Report, Identify Theft Resource Center

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

5

No Industry Immune – All Are Vulnerable

The threats are real.

The risks are high.

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

6

Increasingly today, we have two identities:

A Physical Self

An Information Self

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

7

And our information identities are in harm's way…

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

8

More Risk Factors = More Privacy Risk

Innovations in Technology	• Exponential Increases • Both for Good and Bad • Fast Outpacing Laws
Information Explosion	• Status Quo is not an Option • Internet of Things, Big Data

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

9

More Risk Factors (cont'd.)

Digital Dependence	• Dependence on eCommerce • Commodification of Privacy • Lack of Awareness or Use of Security Controls
Ever-Evolving Laws, Regs, Standards	• Federal, State and Local • EU, Canada, Other Countries • PCI DSS

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

10

More Risk Factors (cont'd.)

Breach and ID Theft	• Not If, But When; No Industry Immune • Stolen Personal Info = $$$ • Cyber Threats are Growing
Reputational Harm	• Stakeholder Expectations • Risk Landscape is Ever-Changing • Brand Management/"Court of Public Opinion"

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

11

By 2019, data breach costs are expected to reach $2.1 trillion!

Lori Widmer, "10 Most Expensive Data Breaches," *Life Health Pro*, June 18, 2015

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

12

Unique Challenges for Higher Education:

- **Create, access, transmit and store large volumes of highly sensitive information.**
- **Repositories of valuable intellectual property.**
- **Privacy and IT security budgets are limited.**
- **IT is often decentralized.**
- **Regulatory defense, fines and penalties divert resources from the mission.**
- **Academic freedom and culture pose challenges to protections.**

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

13

There are 100s of privacy laws and regulations – federal, state, local, global.

Many impact higher education.

Compliance is critical for mitigating risk.

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

14

Applicable Laws, Regulations, Standards, Etc.

- FERPA
- HIPAA/HITECH
- GLBA
- NC IDTPA
- Section 5 of FTC Act
- PCI DSS
- FISMA
- NIST 800-53; 800-171
- Common Rule
- COPPA
- FCRA
- FACTA/Red Flags Rules
- ADA
- OMB Circular A-130
- Privacy Act of 1974
- EU GDPR, and more…

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

15

The steps to mitigating risk…

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

16

IDENTIFY YOUR INFORMATION ASSET LANDSCAPE

Um, excuse me, do what?!

The Daily Information Tsunami!

Students **Staff**
Faculty **Alumni**
Applicants **Subjects**
Patients **Vendors**
Others

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

19

How!?!

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

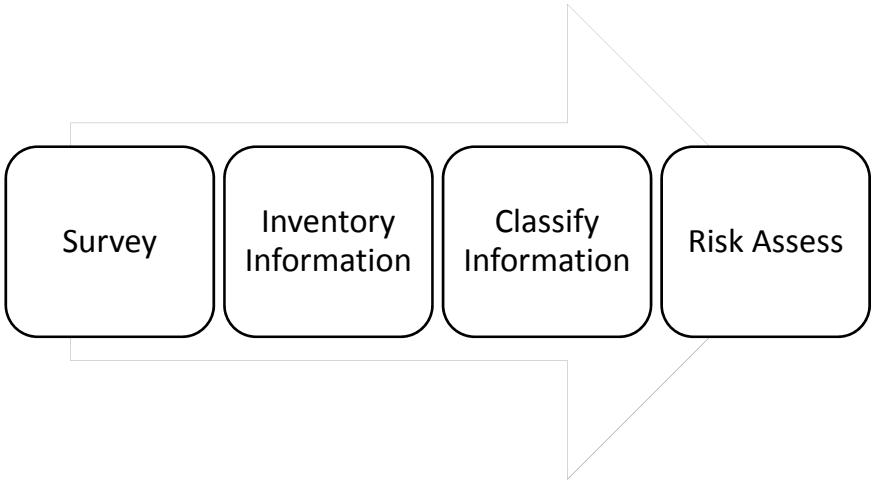
20

How!?! (cont'd.)

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

21

Survey • Inventory • Classify • Risk Assess



Duke | OFFICE of AUDIT, RISK & COMPLIANCE

22

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

23

A Privacy Impact Assessment Identifies

Who is collecting sensitive information	**What is collected**
Why it is collected	**How it is collected, used, accessed, shared, safeguarded and stored**

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

24

A PIA as a Decision Tool:

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 privacy impact assessments or otherwise inventory sensitive data?

The Process

- 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

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

27

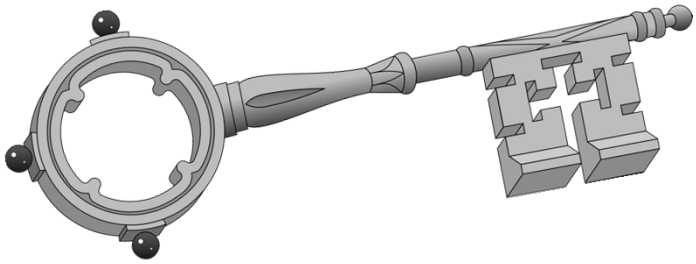
To Further Mitigate Risk and Protect the Institution

Monitor What Comes In, Goes Out and Stays

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

28

Communication is the



to Effective Compliance

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

29

Ensure everyone gets the message!

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

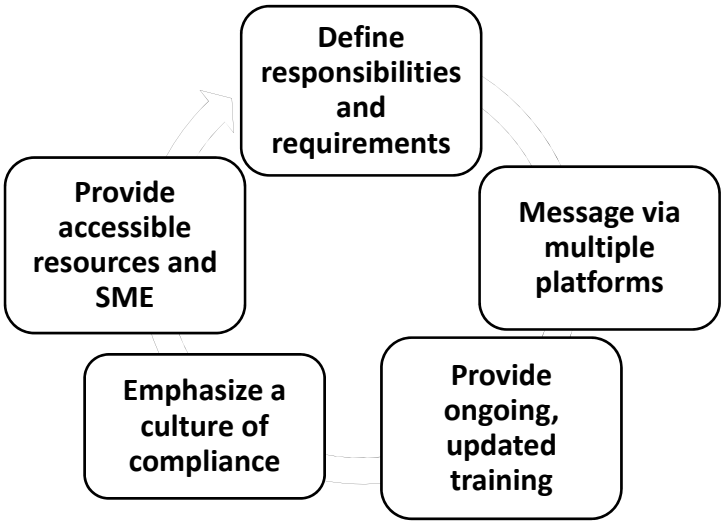
30

How do you communicate?

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

31

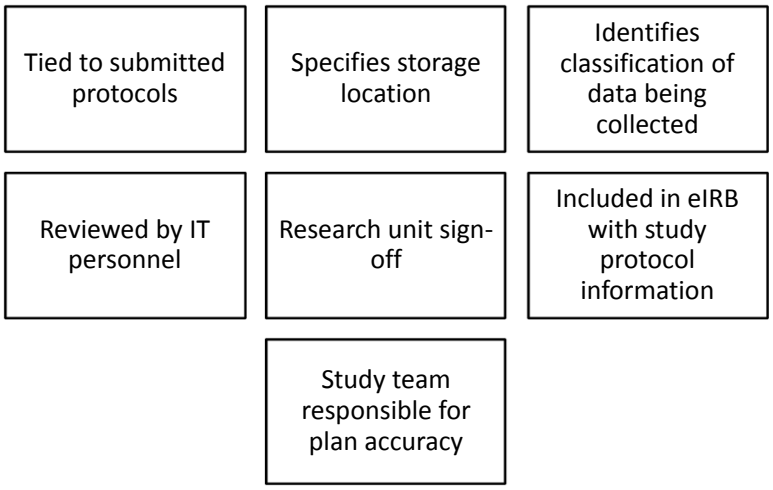
'To Do' List:



Duke | OFFICE of AUDIT, RISK & COMPLIANCE

32

Duke's Research Data Storage Plans (RDSP)



Duke | OFFICE of AUDIT, RISK & COMPLIANCE

33

Example Monitoring Tools:

Data Loss Prevention®

- Monitors sensitive information, such as PHI and financial information, that leaves the institution.
- Auto-encrypts.

FairWarning®

- Privacy software tool that audits EHR and billing access to identify and mitigate impermissible access and disclosures of protected health information.

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

34

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

36

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

37

Activities to Monitor (cont'd.)

- Disclosing PHI without appropriate, executed agreements 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

38

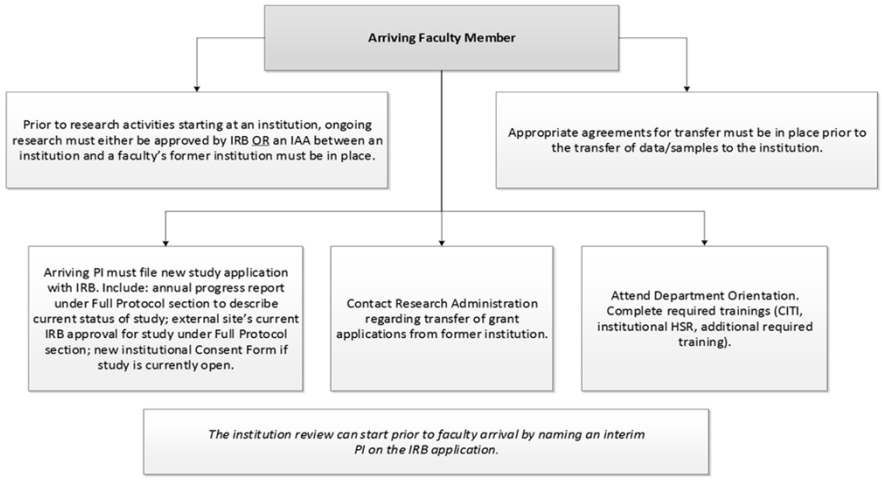
Arriving Faculty

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

39



List of Acronyms:
CITI – Collaborative Institutional Training Initiative
HSR – Human Subjects Research
IAA – IRB Authorization Agreement
IRB – Institutional Review Board
PI – Principal Investigator

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

40

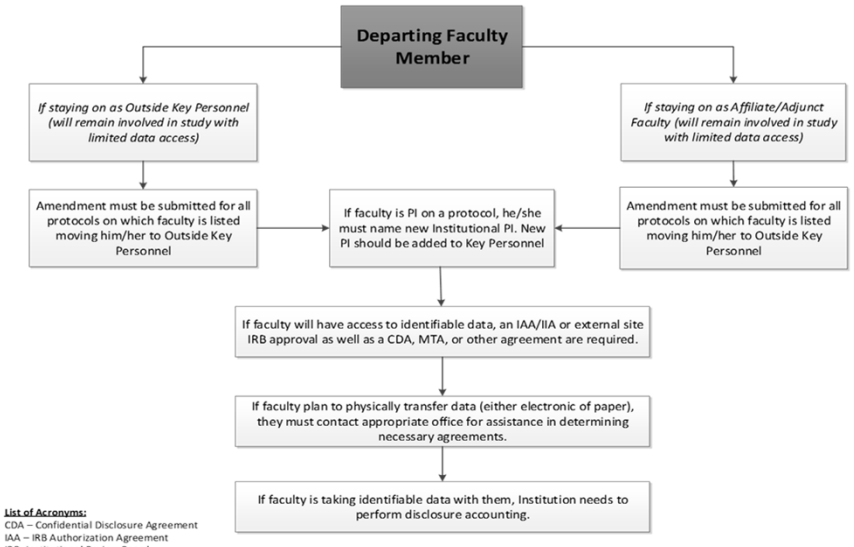
Departing Faculty

Things to Consider:

- Ongoing status on the project
- 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

41

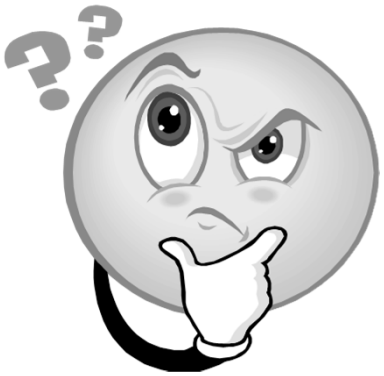


List of Acronyms:
CDA – Confidential Disclosure Agreement
IAA – IRB Authorization Agreement
IRB -Institutional Review Board
MTA – Material Transfer Agreement
PI – Principal Investigator

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

42

Questions?



Duke | OFFICE of AUDIT, RISK & COMPLIANCE

43

Contact information:

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

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

44

Sources

- Images used in this presentation that are not in the public domain are Creative Commons copyrighted and our use is consistent with terms:

  "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; hands holding house image, by Geralt, pixabay.com, CC0; Gold key, by Firkin, openclipart.com, CC0; Brizzle born and bred, free-photos.gatag.net, CC BY-ND; Silent film director D.W. Griffith using megaphone in 1922, unknown photographer, 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

45