HPC, HIPAA, and FISMA: Meeting the Regulatory Challenge through Effective Risk Management

Bill Barnett & Anurag Shankar
Pervasive Technology Institute
Center for Applied Cybersecurity Research
Indiana University

2014 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure
August 26, 2014
Outline

1. Introduction
2. HPC & Compliance at IU: A History
3. HIPAA & FISMA Demystified
4. Cyber Risk Management
5. Building & Leveraging a Risk Management Framework
6. Conclusions
## Schedule

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Introduction</td>
</tr>
<tr>
<td>2.</td>
<td>HPC &amp; Compliance at IU – A History</td>
</tr>
<tr>
<td>3.</td>
<td>A Gentle HIPAA Primer</td>
</tr>
<tr>
<td>4.</td>
<td>A Gentle FISMA Primer</td>
</tr>
<tr>
<td>5.</td>
<td>Cyber Risk Management</td>
</tr>
<tr>
<td>6.</td>
<td>The NIST Risk Management Framework (RMF)</td>
</tr>
<tr>
<td></td>
<td>Break</td>
</tr>
<tr>
<td>7.</td>
<td>Building the NIST RMF at IU</td>
</tr>
<tr>
<td>8.</td>
<td>Using it to address HIPAA</td>
</tr>
<tr>
<td>9.</td>
<td>Conclusions</td>
</tr>
<tr>
<td>10.</td>
<td>Q&amp;A</td>
</tr>
</tbody>
</table>
1. Introduction
HPC & Compliance

- With physical scientists and engineers as primary customers, rules and regulations that govern sensitive data were not relevant to HPC.
- The introduction of expanding health sciences data has pushed HPC out of this comfort zone.
- Suddenly, we find ourselves in a scary & unfamiliar world of regulatory compliance.
The Problem

• Analysis, storage, and management of a growing volume of health sciences research data now requires significant compute resources.

• It is reaching scales typical of data intensive physical sciences and engineering disciplines.

• Medical center IT cannot support projects of this magnitude.

> Users are coming to HPC with clinical data
As cyberinfrastructure leaders managing sensitive Big Data, its about:

Delivering Value – making research happen

Earning Trust – from all our stakeholders

Managing Risk – reimagining security

But it’s really kinda like this…
Weber, Mandl, and Kohane “Finding the Missing Link for Big Biomedical Data” JAMA 2014.4228
Right now, Big Data is still Alchemy

- Omics: new kinds of data with young rules
- Patients as Partners: new stakeholders
- Network Science: new conceptual modes
- Team Science: competitions (Sage/DREAM)
- Crowd Sourcing: public analysis
- Cloud: new data sharing capabilities

Source: Steven Friend, Bio-IT World keynote presentation, April 30, 2014
Compliance Facts

- Clinical research data are subject to HIPAA.
- FISMA is required in govt. grants & contracts.
- IRB’s/Research Administrators/Researchers are neither IT nor regulatory experts so that IT safeguards often do not get addressed as required by government regulations.

→ Breaches & fines
The Regulatory Challenge

- Regulations such as HIPAA & FISMA have their own, specific requirements and stress different areas.
- HPC shops lack regulatory expertise.
- HIPAA fines have increased substantially.
- The government (OCR) has initiated random HIPAA audits in 2014 (Audits occurred only as part of data breach investigations earlier).
No Plausible Deniability

• The service must be HIPAA aligned *if even a single clinical researcher* has an account on the system.

• There is no plausible deniability in HIPAA. It says that you *should have expected* that allowing clinical researchers on the system will lead to clinical data on the system.
2. HPC and Compliance at IU: A History
IU’s HPC Organization

- Indiana University (IU) has provided mature HPC services for many years.
- They are delivered through the Research Technologies (RT) division of the University Information Technology Services (UITS), part of the Pervasive Technology Institute.
- RT provides supercomputing, data storage/archival, visualization, application development and optimization, data management, and other services.
HIPAA History

- IU’s research cyberinfrastructure, like elsewhere, was used mostly by physical scientists and engineers prior to 2000.

- A Lilly Endowment grant accelerated genomics research at IU & established need for HPC services for the IU School of Medicine.

> There was initially no uptake in HPC
Contributing Factors

1. Researchers would not de-identify data (#1 reason for lack of user interest)

2. A mismatch between HPC & medical culture

3. Our lack of regulatory expertise and practice

4. A lack of resources to address 2 & 3
Timeline

- Our HIPAA efforts began in 2007.
- An institution-wide committee for oversight and advocacy.
- An external consultant for gap and risk assessment.
- The project received dedicated resources in 2008.
- Adopted NIST 800-53 as the security standard
- IU Compliance finally deemed us capable of ‘sufficiently protecting ‘ research ePHI in 2009.
- Now moving to FISMA framework for broader application
HIPAA Implementation Steps

1. Assign ownership
2. Form partnerships
3. Document everything
4. Hire external consultant
5. Perform gap analysis/fill gaps
6. Assess risk
7. Create & execute risk management plan
8. Get official blessing & advertise
Steps

① **Assign ownership**: One RT director and one staff (about 1 FTE)
② **Form partnerships**: Put all stakeholders on an oversight committee.
③ **Document everything**: Policies & procedures, responsibilities
④ **Hire external consultant**: Recommended by IU Compliance
⑤ **Perform gap analysis**: Measured how far we are from HIPAA
⑥ **Fill gaps**: Plugged as many holes as we could
⑦ **Assess risk**: Output from 3&5 informed the assessment
⑧ **Create & execute risk management plan**: Guided by consultant
⑨ **Get official blessing & advertise**: Focus on biomedical researchers
### Measures of Success

- **Starting from zero in 2009, we now have:**

<table>
<thead>
<tr>
<th>Measure</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Number of biomedical user accounts</td>
<td>3,000</td>
</tr>
<tr>
<td>2. Volume of biomedical data stored</td>
<td>~1PB</td>
</tr>
<tr>
<td>3. Use of computing cycles</td>
<td>1 MSUs</td>
</tr>
<tr>
<td>4. Number of databases</td>
<td>&gt; 800</td>
</tr>
<tr>
<td>5. New services for biomedical users</td>
<td>&gt; 10</td>
</tr>
<tr>
<td>6. Number of NIH grants that fund us</td>
<td>5</td>
</tr>
<tr>
<td>7. Number of FTEs funded by these grants</td>
<td>~ 10</td>
</tr>
</tbody>
</table>
3. HIPAA & FISMA DEMYSTIFIED
HIPAA

“No, it’s not a female Hippopotamus, anyone else know?”
A Gentle HIPAA Primer

• **Health Insurance Portability & Accountability Act.**


• Enforced by the Office for Civil Rights (OCR) in the US Dept. of Health & Human Services (DHHS).

• The **Omnibus Final Rule** of 2013 includes provisions from the 2006 Health Information Technology for Economic & Clinical Health (HITECH) Act & the 2008 Genetic Information Nondiscrimination Act (GINA).
Patient Privacy Protection

• Addressed via the HIPAA Privacy Rule and the HIPAA Security Rule.

• The Privacy Rule defines who HIPAA applies to (covered entities), what is protected (protected health information or PHI), and covers disclosure.

• The Security Rule focuses exclusively on how to protect electronic PHI (ePHI) in any form – at rest, in transit, under analysis, etc.

  → ePHI = identifiable patient data with any of 18 identifiers
Somehow your medical records got faxed to a complete stranger. He has no idea what’s wrong with you either.
Identifiers that Make Data PHI

1. Names
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census: (1) the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
4. Telephone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web universal resource locators (URLs)
15. Internet protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic or code

PHI, when properly de-identified, is no longer PHI
Relationship to State Laws

- Many states have their own privacy laws.
- If HIPAA is incompatible with state laws, HIPAA preempts state.
- Except when the state law provides greater privacy protections than HIPAA.
- DHHS makes the determination upon request.
- HIPAA is a floor, not a ceiling.
Covered Entity

• HIPAA applies to a covered entity (CE).
• A covered entity is a healthcare provider, a health plan or a health clearinghouse.
• Universities often choose to be hybrid covered entities, with both non-covered and covered components.
• All HIPAA related issues affect the whole CE. (For instance, the CE faces fines when a HIPAA violation occurs, not an individual.)
Am I covered?

• Your organization (say HPC Center) is not a covered entity if you are not involved in healthcare operations directly.
• However, it is still subject to HIPAA if both of the following are true:
  • you serve a covered entity, either as a unit of your covered entity or as a Business Associate, and
  • if you handle ePHI in any way, shape, or form.
• So you cannot say “I didn’t know we had ePHI”.

You are not a covered entity if you are not involved in healthcare operations directly.
A HIPAA Business Associate (BA) is defined as “a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information.”
Business Associate Agreements

- HIPAA requires a Business Associate Agreement (BAA) with BAs that can touch ePHI on your system (since it’s a disclosure).
- The BAA must include language that the BA will protect your ePHI and abide by HIPAA. (Sample BAAs at DHHS site.)
- You must do due diligence (an assessment) to ensure that the BA can protect your ePHI as per HIPAA.
Am I a Business Associate?

- You are **not** a BA if you are part of a university and provide services to its medical school or other covered components.
- You **are** if you provide services to an external covered entity. Then the CE **must** have a HIPAA BAA with you (since your sys admins have access to their user data/ePHI).
- They are in violation of HIPAA if they do not.
Recent HIPAA Changes

- The HIPAA Omnibus Final Rule added HITECH & GINA provisions, new business associate & breach notification requirements, and audits/enforcement.
  - HITECH was part of ARRA and enacted to promote the adoption of Health Information Technology, especially Electronic Health Records (EHR).
  - GINA prohibits insurers from using human genetic data to deny coverage based on genetic predisposition to future diseases. However, genetic data without the 18 identifiers is not subject to HIPAA.
HIPAA after Omnibus

HIPAA Omnibus Rule: Enforces HITECH and applies HIPAA Compliance to Business Associates © 2014 PointClear Solutions, Inc.
Are genetic data ePHI?

- NO, so long as it is not tied to a person using one of the 18 identifiers. This is true even though it is possible in principle to identify a person using unidentified genetic data alone.
- However, the risk is low since such identification is no easy task.
- Note that rules governing human subjects still apply.
- Keep monitoring the legal landscape for changes.
Breach Notification

- HIPAA requires that a breach of ePHI be reported to the OCR & those affected within 60 days.
- For breaches involving > 500 individuals, local media outlets must also be notified.
- You must use your local IT incident reporting mechanism to create an official record of your response for audit purposes.
Enforcement

- HIPAA is enforced by the Office for Civil Rights (OCR) in the Dept. of Health & Human Services (DHHS).
- Violations can result in civil monetary penalties (up to $1.5 million) against a covered entity and/or individual criminal penalties (imprisonment up to 10 years).
- The OCR was funded via ARRA/HITECH to institute an audit program. They have done 150 audits already and getting ready for more.
Civil Monetary Penalties

<table>
<thead>
<tr>
<th>Violation Category</th>
<th>Each Violation</th>
<th>All Identical Violations Per Calendar Year</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>For violations occurring before 2/18/2009</td>
<td>For violations occurring after 2/18/2009</td>
</tr>
<tr>
<td>Did Not Know</td>
<td>Up to $100</td>
<td>$100 - $50,000</td>
</tr>
<tr>
<td>Reasonable Cause*</td>
<td>Up to $100</td>
<td>$1000 - $50,000</td>
</tr>
<tr>
<td>Willful Neglect - Corrected</td>
<td>Up to $100</td>
<td>$10,000 - $50,000</td>
</tr>
<tr>
<td>Willful Neglect - Not Corrected</td>
<td>Up to $100</td>
<td>$50,000</td>
</tr>
<tr>
<td></td>
<td>For violations occurring before 2/18/2009</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For violations occurring after 2/18/2009</td>
<td></td>
</tr>
<tr>
<td>Reasonable Cause*</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>$25,000</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>

* = An act of omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification (HIPAA) provision, but in which the covered entity or business associate did not act with willful neglect.

The cost of “I didn’t know we had ePHI”.

[HIPAA logo]
Wonders of Multiplication

- HIPAA penalties are levied per violation.
- Breach of an individual record is one violation. To calculate your total, multiply by the number of affected individuals.
- Fortunately, there are maximums. Still, these are serious numbers.
- The worst hit you take is not the penalty but damage to the institution’s reputation.
HIPAA Civil/Criminal Penalties in Action

- WellPoint to pay $1.7 million HIPAA penalty
- Group slapped with $6.8M HIPAA fine
- $400,000 Penalty in HIPAA Case
- Another Big Fine After a Small Breach
- Stanford reports fifth big HIPAA breach
- $4.8M HIPAA Fine Part Of Wider HHS Crackdown
- HHS attorney predicts big year for HIPAA fines
- Alaska settles HIPAA security case for $1,700,000
- Walgreens must pay woman $1.44 million over HIPAA violation
- New York-Presbyterian, Columbia to pay largest HIPAA settlement: $4.8 million
- HIPAA Breaches in the Cloud
- 2 Oregon Incidents Reveal Omnibus Fog
- New York-Presbyterian, Columbia to pay largest HIPAA settlement: $4.8 million
- HIPAA Violation Indictments for 2 Medical Office Assistants
- United States Attorney and U.S. Secret Service announced indictment of twelve individuals in a
The absolute worst is being in the newspapers!

Breaches reported by universities

ISU settles HIPAA security case for $400,000

RESOLUTION AGREEMENT

I. Recitals

1. Parties. The Parties to this Resolution Agreement (Agreement) are the United States Department of Health and Human Services, Office for Civil Rights (HHS) and Idaho State University (ISU).

2. Authority of HHS. HHS enforces the Federal standards that govern the privacy of individually identifiable health information (45 C.F.R. Part 160 and Subparts A and E of Part 164, the “Privacy Rule”) and the Federal standards that govern the security of electronic individually identifiable health information (the “Security Rule”). HHS investigated ISU’s compliance with the Privacy Rule and Security Rule. HHS’ investigation indicated that the following conduct occurred (“Conduct”).

   i. ISU did not conduct an analysis of the risk to the confidentiality of ePHI as part of its security management process from April 1, 2007 until November 26, 2012.

   ii. ISU did not adequately implement security measures sufficient to reduce the risk and vulnerabilities to a reasonable and appropriate level from April 1, 2007 until November 26, 2012; and

   iii. ISU did not adequately implement procedures to regularly review records of information system activity to determine if any ePHI was used or disclosed in an inappropriate manner from April 1, 2007 until June 6, 2012.

3. Factual Background and Covered Conduct. On August 9, 2011, HHS received notification from ISU regarding a breach of its unsecured electronic protected health information (ePHI). On November 22, 2011, HHS notified ISU of its investigation regarding ISU’s compliance with the Privacy Rule and Security Rule. HHS’ investigation indicated that the following conduct occurred (“Covered Conduct”).

   i. ISU did not conduct an analysis of the risk to the confidentiality of ePHI as part of its security management process from April 1, 2007 until November 26, 2012.

   ii. ISU did not adequately implement security measures sufficient to reduce the risk and vulnerabilities to a reasonable and appropriate level from April 1, 2007 until November 26, 2012; and

   iii. ISU did not adequately implement procedures to regularly review records of information system activity to determine if any ePHI was used or disclosed in an inappropriate manner from April 1, 2007 until June 6, 2012.

4. No Admission. This Agreement is not an admission of liability by ISU.

5. No Concession. This Agreement is not a concession by HHS that ISU is not in violation of either the Security Rule and the Security Rule and that ISU is not liable for civil money penalties.

6. Intent of Parties to Effect Resolution. This Agreement is intended to resolve HHS Transaction Number: 11-135876, and any violations of the HIPAA Privacy and Security Rules for the Covered Conduct specified in paragraph 3 of this Agreement. In consideration of the Parties’ interest in avoiding the uncertainty, burden and expense of further investigation and formal proceedings, the Parties agree to resolve this matter according to the Terms and Conditions below.

II. Terms and Conditions

7. Payment. ISU agrees to pay HHS the amount of $400,000 (Resolution Amount). ISU agrees to pay the Resolution Amount by electronic funds transfer pursuant to written instructions to be provided by HHS. ISU agrees to make this payment within 10 days of the Effective Date.
What happens after a breach?

- The OCR, affected individuals, and/or media are notified.
- All documentation (incident response, policies & procedures, risk assessment, management, etc.) is submitted to OCR.
- OCR may open an investigation or bless due diligence if response is swift and addresses underlying risks.
- Or it may require a “Corrective Action Plan” (CAP) and levy a fine.
- If appropriate, a CAP response is submitted to OCR.
- OCR closes the investigation.
Breach Investigation

During an investigation, the OCR looks for:

- **Documented Policies & Procedures**
- **Implementation of Policies & Procedures**
- **Internal investigation reports, interview statements, etc.**
- **Appropriate sanctions applied**

- **Documented Training**
- **Business Associate Agreements**
- **Documented Risk assessment, mitigation**
- **Encryption & mobile device policies/implementati on**
Protecting ePHI: The HIPAA Security Rule
The HIPAA Security Rule

- The Security Rule requires 1. Administrative, 2. Physical, and 3. Technical safeguards to:
  - Ensure the confidentiality, integrity, and availability of all ePHI created, received, maintained or transmitted;
  - Identify and protect against reasonably anticipated threats to the security or integrity of the information;
  - Protect against reasonably anticipated, impermissible uses or disclosures;
  - Ensure compliance by the workforce; and
  - Provide a means for managing risk in an ongoing fashion.
Security Rule Safeguards

• **Administrative** – security management/officer, workforce security, access management, incident response, disaster planning, evaluations, etc.

• **Physical** – facilities access, workstation use/security, device/media controls.

• **Technical** – access/audit control, integrity, authentication, transmission security.

  + organizational/policies/documentation requirements
Required & Addressable

- Each Security Rule safeguard is either required or addressable.
- Required = what it says.
- Addressable = should address, but ok if you describe why it is not in place or how you will otherwise address the risk.
- A risk assessment (RA) identifies where to concentrate your HIPAA effort.
Standards and Implementation

• The Security Rule defines a standard and specifies its implementation specifications.

• Standards address broad categories.
• Implementation specifications are just what it says; how they are to be implemented.
• It’s the implementation specifications that are either required or addressable.

(5)(i) Standard: Security awareness and training. Implement a security awareness and training program for all members of its workforce (including management).
(ii) Implementation specifications. Implement:
(B) Protection from malicious software (Addressable). Procedures for guarding against, detecting, and reporting malicious software.
(C) Log in monitoring (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.
(D) Password management (Addressable). Procedures for creating, changing, and safeguarding passwords.
(E) Standard: Security audit.
Does HIPAA apply to all Identifiable Health Data?

- **NO.** Only healthcare providers, facilities, and insurers are bound by HIPAA. Identifiable health data outside of a healthcare context is not ePHI.
- Data, if properly de-identified, is not subject to HIPAA.

→ If unsure, contact your HIPAA Compliance office.
Who is HIPAA implicated in my organization?

- Employees, healthcare providers, trainees & volunteers at the medical school and affiliated healthcare sites or programs.
- Employees who work with university health plans.
- Employees who provide financial, legal, business, administrative, or IT support to the above.
Q: So, the HIPAA Security Rule means we just need to provide good IT security for systems?

A: NO. The Security Rule is about managing risk, and security is only PART of that management. HIPAA requires administrative controls, training, governance, policies, formal review, etc.
Do I firewall & encrypt it all?

- **MAYBE.** The Security Rule does not prescribe particular solutions or specifications, only broad guidelines, to be interpreted by individual implementers according to their environments.
- It requires a managed risk approach that proves **due** and ongoing diligence.
- Documentation is **key.** If it is not documented **IN DETAIL,** it doesn’t exist as far as OCR is concerned.
Encryption & Safe Harbor

- Encryption is not a required HIPAA Security Rule safeguard.
- However, it is highly recommended, both in transit and at rest.
- If the data is encrypted at rest and the encryption key is stored separately from the data, a breach need not be reported to the OCR.
- This is called “safe harbor”.
Local Risk Tolerance

• Since HIPAA gives such wide berth, it is typically your institutional risk tolerance that in reality determines what you must do.

• Some build walled gardens; we didn’t.

• Instead, we had our HIPAA Privacy and Security Officers oversee the establishment of a risk management process.

• We/they feel that we do sufficient due diligence and can survive an audit.
What exactly is HIPAA Security Rule Compliance?
Unfortunately, this is not too practical – information needs sharing to be useful
Typical Presumptions

• That HIPAA compliance is a boolean = there is a threshold which, when crossed, make you compliant.
• That you can have a qualified third party review your environment and certify your HIPAA compliance.
• That the whole compliance exercise is a one time deal.

That's not true!
Here is what the DHHS says:

**Health Information Privacy**

**Are we required to “certify” our organization’s compliance with the standards of the Security Rule?**

**Answer:**

No, there is no standard or implementation specification that requires a covered entity to "certify" compliance. The evaluation standard § 164.308(a)(8) requires covered entities to perform a periodic technical and non-technical evaluation that establishes the extent to which an entity's security policies and procedures meet the security requirements. The evaluation can be performed internally by the covered entity or by an external organization that provides evaluations or "certification" services. A covered entity may make the business decision to have an external organization perform these types of services. It is important to note that HHS does not endorse or otherwise recognize private organizations’ "certifications" regarding the Security Rule, and such certifications do not absolve covered entities of their legal obligations under the Security Rule. Moreover, performance of a "certification" by an external organization does not preclude HHS from subsequently finding a security violation.

→ You can only establish the extent to which you are compliant. We therefore use the word “aligned” rather than “compliant”.
HIPAA Compliance Facts

• There is nothing that assures that you are 100% compliant. The OCR may still find you lacking.

• Except for one way - an OCR audit! This however is really not a choice. Due diligence is easier.

• So you read the Security Rule carefully, do your best to implement the requisite administrative, physical, and technical safeguards, and self-assert compliance.
The Boon and Bane of HIPAA

HIPAA Security Rule is wonderfully broad and flexible. Unfortunately, this greatly frustrates IT folks who first encounter it because they can’t figure out exactly what is required of them.

"Ok, so it’s carved in stone, but still open to interpretation, right?"
The HIPAA Security Rule Fundamentals

- Risk Analysis
- Information System Activity Review
- Risk Management
- Sanctions Policy
HIPAA Security Rule Process

- There are many ways to do HIPAA, based on your environment, budget, and risk tolerance.
- Your local HIPAA Compliance or Information Security folks may already have a process in place so check with them first.
- Instead of covering details here, we’ll illustrate it later using a standards based risk management approach.
Some HIPAA Stats
Breach Notification Stats as of 2/14: 500+ Breaches by Type

- Theft: 48%
- Unauthorized Access/Disclosure: 18%
- Loss: 11%
- Other: 10%
- Unknown: 1%
- Improper Disposal: 5%
- Hacking/IT Incident: 7%

Courtsey Linda Sanchez, OCR
Breach Notification Stats as of 2/14: 500+ Breaches by Location

- Laptop: 23%
- Paper Records: 22%
- Desktop Computer: 14%
- Portable Electronic Device: 12%
- Other: 10%
- EMR: 4%
- Network Server: 11%
- E-mail: 4%

Courtesy Linda Sanchez, OCR
Lessons from Breaches

• Most of the breaches occur due to theft/loss & improper disclosure.

• Hacking or IT incidents is only at 7%. However, even one breach at our end is too many since it can be highly damaging to the CE.

• A lot of breaches occur at the user end & have to do with (unencrypted) mobile devices. Paper records are still big.
Top Areas of Weakness Revealed by Breach Stats

- User Activity Monitoring
- Contingency Planning
- Authentication and Integrity
- Media Reuse and Destruction
- Risk Assessments
- Granting or Modifying Access
Lessons from Recent OCR Audits

- No risk assessments
- Improper media movement and disposal
- No/inadequate audit controls and monitoring
FISMA
A Gentle FISMA Primer

Federal Information Security Management Act of 2002

“Each federal agency shall develop, document, and implement an agency wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source …”
FISMA Requirements

- All government agencies must secure their system as per NIST guidelines.
- Universities accepting government contracts must also comply (similar to the HIPAA BA rule).
- In fact, grants & contracts are already beginning to include FISMA language, especially from NIH.

→ It is time to start getting ready.
When does FISMA Apply?

- When you use your systems to collect or maintain information on behalf of the agency (e.g. for a grant or contract).
- When you use or operate information systems on behalf of the agency (e.g. a cloud provider).
- The contract or grant will explicitly state FISMA terms. If not, count your lucky stars.
- New FISMA language may be added to existing contracts so be sure to check that too.
FISMA is hard!

- FISMA will require a budget.
- You will need FTEs to handle FISMA.
- You will need to create an administrative process.
- You may have to create a FISMA walled garden.
- You will need patience.

However, it is often possible to negotiate things to something acceptable to both sides.
The FISMA Process

- Starts with FISMA language in a grant/contract.
- Triggers a local administrative process.
- Requires appropriate (NIST) documentation.
- The local administrative unit submits FISMA paperwork to the agency.
- The agency responds.
- Remediation may be required and more paperwork submitted.
- The agency issues an “Authority to Operate” (ATO) the system.
Local Administrative Process

- Grants Administrators/Business Development
  - Identify and notify Research Administration of FISMA terms in contract
  - Make sure the budget includes FISMA costs
  - Identify and document key IT security personnel
  - Make sure all documents that are referenced are included

- PI/Study Team
  - Clearly describe the scope of work
  - Identify all potential subcontractors and their scope of work

- PI/Study Team and IT Team
  - Identify authorization boundary
  - Apply NIST RMF
FISMA Authorization Boundary

- Also known as the “accreditation boundary”.
- Defines where the system begins and ends.
- A system can be a part of a network, an application, a logically connected collection of disparate components, etc.
- The authorization boundary extends to all direct and indirect users of the system that receive output.
- Requires IT professionals to identify.
Real Life Academic Implementations

- IU does not have a formal FISMA process in place yet. We’re doing case studies at other institutions.
- Of particular interest is Duke Medicine which has a relatively robust FISMA process.
- They have built an IaaS based, external FISMA hosting environment.
- But, FISMA burdens are such that Duke won’t accept FISMA High contracts.
What it takes to FISMA

• Duke estimates that, for each contract, it takes them 23-25 hours to review all documentation, make suggested contractual changes for agency negotiation, and create a FISMA management plan.
• To handle FISMA, you must first learn NIST and be ready to negotiate.
• If you don’t have a FISMA implementation, don’t accept FISMA contracts or talk to the agency.
FISMA Fines?

• Unlike HIPAA, which is enforced via civil monetary penalties, FISMA does not have a defined sanction structure.
• Federal agencies are penalized through censure by congress, public scorn, and reduced funding.
• The worst for university grants & contracts is that you will lose the contract and/or won’t get any new ones.
FISMA Reporting

• Unlike HIPAA, FISMA requires quarterly and annual reports to the agency.

• It includes reporting
  • updates to the system security plan to reflect the proposed or actual changes to the information
  • updates to the plan of action and milestones based on the activities carried out during the continuous monitoring phase
  • the security status of the information system.
There's even a HIPAA to FISMA Crosswalk

An Introductory Resource Guide for Implementing the HIPAA Security Rule

**Appendix E—HIPAA Security Rule/FISMA Requirements Crosswalk**

This appendix provides a crosswalk of the Administrative, Technical and Physical standards and implementation specifications of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule to the requirements of the Federal Information Security Management Act of 2002 (FISMA), which contains requirements relevant to the security programs of all federal agencies.

Table E-1. HIPAA Security Rule/FISMA Requirements Crosswalk

<table>
<thead>
<tr>
<th>HIPAA Reference</th>
<th>FISMA Reference</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>164.308(a)(1)(K)</td>
<td>Ref §3544(a)(b)(1)</td>
<td>Periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency.</td>
</tr>
<tr>
<td>164.308(a)(1)(M)(A)</td>
<td>Ref §3544(a)(b)(1)</td>
<td>Periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency.</td>
</tr>
<tr>
<td>164.308(a)(1)(M)(B)</td>
<td>Ref §3544(b)(2)</td>
<td>Policies and procedures that—(A) are based on the risk assessments required by paragraph (1)(B) cost-effectively reduce information security risks to an acceptable level; (C) ensure that information security is addressed throughout the life cycle of each agency information system; and (D) ensure compliance with—(i) the requirements of this subchapter; (ii)</td>
</tr>
</tbody>
</table>

**ADMINISTRATIVE SAFEGUARDS**

- Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations.
- Risk Analysis (R): Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.
- Risk Management (R): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.308(a).
4. Cyber Risk Management
Compliance in research means following the data through its entire research lifecycle and managing cyber risk comprehensively. This includes both the user and the IT provider end.
Managing Cyber Risk

- Identify, assess, prioritize, and mitigate risk to information security on an ongoing basis.
- Makes you think in terms of managing risk, not just plugging system security holes.

Risk = \{\text{Threat/Vulnerability} \times \text{Likelihood} \times \text{Impact}\}

- A big threat from an existing vulnerability that is highly unlikely to be exploited or has little impact is low risk. You don’t kill yourself over it.
Risk Assessment

• ... is like the air you breathe in the information security risk management world. You cannot manage risk without first assessing it.

• There are many ways to assess risk, ranging all the way from pedestrian (& cheap) to highly complex (& expensive).

• Your effort should be commensurate with your budget, risk tolerance, and complexity.
A mature RMF is a complete risk management package. It includes:

- **Governance** = institutional security organization, policies, sanctions, enforcement
- **Risk management** = assessment, mitigation through appropriate physical, administrative, technical controls, documentation
- **Review** = regular monitoring, reviews, assessment, and mitigation
- **Awareness and training** = for both staff and users
Industry Standard RMFs

- NIST RMF = National Institute of Standards and Technology RMF
- DIACAP = Dept. of Defense Information Assurance Certification Process
- OCTAVE = Operationally Critical Threat, Asset, and Vulnerability Evaluation
- HITRUST CSF = Health Information Trust Common Security Framework
- FAIR = Factor Analysis of Information Risk
- TARA = Threat Agent Risk Assessment
The NIST RMF

- Let’s take a detailed look at the NIST RMF.
- It will show that the NIST RMF is comprehensive and yet flexible enough to adapt to any environment/scale.
- The RMF essentially represents a cybersecurity lifecycle.
- The steps are described by NIST and other govt. publications.
NIST Security Lifecycle

Starting Point
FIPS 199 / SP 800-60

- Monitor Security Controls
  SP 800-37
  SP 800-53A

- Authorize Information System
  SP 800-37

- Assess Security Controls
  SP 800-53A

Categorize Information System

- Implement Security Controls
  SP 800-70

Select Security Controls
FIPS 200 / SP 800-52

- Supplement Security Controls
  SP 800-53 / SP 800-30

- Document Security Controls
  SP 800-18

Risk Management Framework
Security Life Cycle
1. Categorize

- FIPS 199 (Standards for Security Categorization of Federal Information and Information Systems) helps categorize data based on confidentiality, integrity, and availability.
- Categories are Low, Medium, and High.
- NIST 800-60 (Guide for Mapping Types of Information and Information Systems to Security Categories) outlines a process for categorization.
## FIPS 199 Categorization

<table>
<thead>
<tr>
<th>Security Objective</th>
<th>Low</th>
<th>Moderate</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Confidentiality</strong></td>
<td>The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</td>
</tr>
<tr>
<td>Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 USC, SEC. 3542]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Integrity</strong></td>
<td>The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</td>
</tr>
<tr>
<td>Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 USC, SEC. 3542]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Availability</strong></td>
<td>The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</td>
</tr>
<tr>
<td>Ensuring timely and reliable access to and use of information. [44 USC, SEC. 3542]</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
2. Select Controls

- FIPS 200 (Minimum Security Requirements for Federal Information and Information Systems) ties minimums to the NIST 800-53 controls.
- NIST 800-53 (Security & Privacy Controls for Federal Information Systems and Organizations) provides a catalog of security controls. They are divided into control families. Each controls has a baseline and zero or more control enhancements for stricter security.
Table D-2 provides a summary of the security controls and control enhancements from Appendix F that have been allocated to the initial security control baselines (i.e., low, moderate, and high). The sequence priority codes for security control implementation and those security controls that have been withdrawn from Appendix F are also indicated in Table D-2. In addition to Table D-2, the sequence priority codes and security control baselines are annotated in a priority and baseline allocation summary section below each security control in Appendix F.

<table>
<thead>
<tr>
<th>CNTL NO.</th>
<th>Control Name</th>
<th>Priority</th>
<th>INITIAL CONTROL BASELINES</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access Control Policy and Procedures</td>
<td>P1</td>
<td>AC-1 AC-1 AC-1 AC-1</td>
</tr>
<tr>
<td></td>
<td>Account Management</td>
<td>P1</td>
<td>AC-2 AC-2 (1) (2) (3) (4)</td>
</tr>
<tr>
<td></td>
<td>Access Enforcement</td>
<td>P1</td>
<td>AC-3 AC-3 AC-3 AC-3</td>
</tr>
<tr>
<td></td>
<td>Information Flow Enforcement</td>
<td>P1</td>
<td>Not Selected AC-4 AC-4</td>
</tr>
<tr>
<td></td>
<td>Separation of Duties</td>
<td>P1</td>
<td>Not Selected AC-5 AC-5</td>
</tr>
<tr>
<td></td>
<td>User Privilege</td>
<td>P1</td>
<td>Not Selected AC-6 AC-6</td>
</tr>
<tr>
<td></td>
<td>Unsuccessful Logon Attempts</td>
<td>P2</td>
<td>AC-7 AC-7 AC-7 AC-7</td>
</tr>
<tr>
<td></td>
<td>System Use Notification</td>
<td>P1</td>
<td>AC-8 AC-8 AC-8</td>
</tr>
<tr>
<td></td>
<td>Previous Login (Access) Notification</td>
<td>P1</td>
<td>Not Selected Not Selected Not Selected AC-9</td>
</tr>
<tr>
<td></td>
<td>Concurrent Session Control</td>
<td>P2</td>
<td>Not Selected AC-10</td>
</tr>
<tr>
<td></td>
<td>Session Lock</td>
<td>P3</td>
<td>Not Selected AC-11 (1)</td>
</tr>
<tr>
<td></td>
<td>Session Termination</td>
<td>P2</td>
<td>Not Selected AC-12</td>
</tr>
<tr>
<td></td>
<td>Withdrawn</td>
<td>P2</td>
<td>AC-13 AC-13 AC-13 AC-13</td>
</tr>
<tr>
<td></td>
<td>Permitted Actions without Identification or Authentication</td>
<td>P2</td>
<td>AC-14 AC-14 AC-14 AC-14</td>
</tr>
<tr>
<td></td>
<td>Withdrawn</td>
<td>P2</td>
<td>AC-15 AC-15 AC-15 AC-15</td>
</tr>
<tr>
<td></td>
<td>Security Attributes</td>
<td>P2</td>
<td>Not Selected Not Selected Not Selected</td>
</tr>
<tr>
<td></td>
<td>Remote Access</td>
<td>P1</td>
<td>AC-16 AC-16 AC-16 AC-16</td>
</tr>
<tr>
<td></td>
<td>Wireless Access</td>
<td>P1</td>
<td>AC-17 AC-17 AC-17 AC-17</td>
</tr>
<tr>
<td></td>
<td>Access Control for Mobile Devices</td>
<td>P1</td>
<td>AC-18 AC-18 AC-18 AC-18</td>
</tr>
<tr>
<td></td>
<td>Use of External Information Systems</td>
<td>P1</td>
<td>AC-19 AC-19 AC-19 AC-19</td>
</tr>
<tr>
<td></td>
<td>Information Sharing</td>
<td>P2</td>
<td>AC-20 AC-20 AC-20 AC-20</td>
</tr>
<tr>
<td></td>
<td>Publicly Accessible Content</td>
<td>P2</td>
<td>AC-21 AC-21 AC-21 AC-21</td>
</tr>
<tr>
<td></td>
<td>Data Mining Protection</td>
<td>P2</td>
<td>AC-22 AC-22 AC-22 AC-22</td>
</tr>
<tr>
<td></td>
<td>Access Control for Access Control</td>
<td>P2</td>
<td>AC-23 AC-23 AC-23 AC-23</td>
</tr>
<tr>
<td></td>
<td>Awareness and Training Policy and Procedures</td>
<td>P1</td>
<td>AT-1 AT-1 AT-1 AT-1</td>
</tr>
</tbody>
</table>

The control family baselines in Table D-2 are the initial baselines selected by organizations prior to conducting the table activities described in Section 3.2. The control baselines and priority codes are solely applicable to non-national security systems. Security control baselines for national security systems are included in CSSS Instruction 1232.

Reference: NIST Special Publications 800-12, 800-100.
Control Enhancements:

1. **Least Privilege | Authorize Access to Security Functions**
   - The organization explicitly authorizes access to [Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information].
   - **Supplemental Guidance**: Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users. Related controls: AC-2, AC-3, AC-5, CM-6, CM-7, PL-2.

2. **Least Privilege | Non-Personnel Access to Nonsecurity Functions**
   - The organization requires that users of information system accounts, or roles, with access to [Assignment: organization-defined security functions or security-relevant information], use non-privileged accounts or roles, when accessing nonsecurity functions.
   - **Supplemental Guidance**: This control enhancement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account. Related control: PL-4.

3. **Least Privilege | Network Access to Privileged Commands**
   - The organization authorizes network access to [Assignment: organization-defined privileged commands] only for [Assignment: organization-defined compelling operational needs], and documents the rationale for such access in the security plan for the information system.
   - **Supplemental Guidance**: Network access in any access across a network connection in lieu of local access (i.e., user being physically present at the device). Related control: AC-17.

4. **Least Privilege | Separate Processing Domains**
   - The information system provides separate processing domains to enable finer-grained allocation of user privileges.
   - **Supplemental Guidance**: Providing separate processing domains for finer-grained allocation of user privileges includes, for example: (i) using virtualization techniques to allow additional privileges within a virtual machine while restricting privileges to other virtual machines or to the underlying hardware; (ii) employing hardware- and/or software-domain separation mechanisms; and (iii) implementing separate physical domains. Related controls: AC-4, SC-3, SC-30, SC-32.

5. **Least Privilege | Privileged Accounts**
   - The organization restricts privileged accounts on the information system to [Assignment: organization-defined personnel or roles].
   - **Supplemental Guidance**: Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial-off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information functions. Organizations may differentiate in the application of this control enhancement between allowed privileges for local accounts and for domain accounts provided organizations retain the ability to control information.
Control Selection

- If you are aligning with the NIST Low security baseline, you select from the controls that are in the “LOW” column.
- More and more controls must be added as you move to Moderate and High baselines.
- FISMA Low, Moderate, and High correspond to the NIST Low, Moderate, and High baselines.

800-53 has 936 total controls, with 16 covering program management, 240 base, and 680 enhancements.
3. Supplement Controls

- Controls are supplemented as needed to mitigate risks after a risk assessment identifies them.
- NIST 800-30 (Guide for Conducting Risk Assessments) provides the steps to carry out a risk assessment.
- NIST risk assessment is based on threat/vulnerability/likelihood/impact determination. It can be as simple or as complex as needed.
NIST Risk Assessment & Response

- Step 1: System Categorization
- Step 2: Threat Identification
- Step 3: Vulnerability Identification
- Step 4: Control Analysis
- Step 5: Likelihood Determination
- Step 6: Impact Analysis
- Step 7: Risk Determination
- Step 8: Control Recommendations
- Step 9: Results Documentation
Risk Assessment/Response Documentation

- The risk assessment process is documented in a Risk Assessment report. It describes the methodology used, areas of risk and vulnerabilities, and severity.
- The response is documented in what is called the Plan of Action & Milestones (POA&M).
- It documents risk response - whether the risk was accepted, mitigated, or transferred to someone else. It also specifies timelines and actions for mitigation as appropriate.
4. Document Controls


- The SSP describes system details and documents every NIST 800-53 security and privacy control currently in place, both base and enhancements.

- It is the most voluminous NIST document and requires some knowledge of NIST 800-53.
5. Assess Controls

• NIST 800-53A (Guide for Assessing the Security Controls in Federal Information Systems & Organizations) describes how to develop a plan to assess desired security controls.

• It helps build assurance into the RMF.

• The organization is left to devise the tests that assess the controls. Examples are penetration testing to break into systems, etc.
6. Authorize Information System

• NIST 800-37 (Guide for Applying the Risk Management Framework to Federal Information Systems) describes how to leverage the NIST RMF once it is in place. It describes all of the NIST steps in detail.

• Authorization is based upon the information in the authorization package, namely the POA&M, the SSP, and the RA report.
7. Monitor Information System

• NIST 800-37 also describes how security controls should be monitored on an ongoing basis for system changes & their impact.

• It provides guidance on regular security/risk assessments, remediation, system removal, decommissioning, etc.

• Continuous monitoring is an essential requirement of FISMA.
Compliance & Clouds
How are we doing?

• Both the government and cloud vendors have struggled with compliance.
• Most vendors refuse to sign a HIPAA BAA, largely due to liability and/or ignorance. Fortunately, the majors - AWS, Microsoft, Box, etc. - will now sign.
• There is also a program called FedRAMP that a cloud vendor can go through to comply with FISMA. It is not easy!
HIPAA in the Cloud

• It is finally possible to use the cloud to store or process ePHI.
• We have just subjected Box to a HIPAA assessment and will soon allow researchers to use it for ePHI.
• Most cloud vendors are simply choosing to encrypt all data at rest and in transit to lower risk.
• There are also vendors who will provide a HIPAA “compliant” hosting environment.
5. Building & Leveraging a Risk Management Framework
Where to start?

- At first glance, HIPAA and FISMA seem highly onerous.
- Digging deeper shows that this is not necessarily true.
- Because you already have many components of a RMF in place (whether or not you realize it).
- This becomes clear when you start taking stock
- If you don’t believe it, let me prove it to you.
Pre-existing RMF Components

• Administrative controls - institutional policies & procedures, disaster recovery, incident response, workforce security, training, etc.
• Physical controls – secure data center, etc.
• Technical controls – access control, account management, logging, patching, backups, encryption (ssh, https), firewalls, monitoring, etc.
• Documentation
Choosing a RMF

• You can choose from any number of cybersecurity RMFs available these days.
• FAIR is a good one at modest scales.
• OCTAVE provides an organizational RMF.
• NIST is good for HIPAA and especially good if you are considering FISMA.
• We chose NIST because pretty much any govt. or other rule/regulation can be mapped to NIST.
Building the RMF at IU

• The only real world RMF we can illustrate is ours.
• It is NIST based and is used to handle HIPAA currently.
• We hope to use it for FISMA and other rules and regulations going forward.
• The idea is to create a standards based foundation for all cyber compliance at IU.
• The project started about a year ago, took 1 FTE, and completed recently.
IU’s NIST RMF Implementation

• Our NIST implementation is lightweight and nimble – we decided to start simple and align with the NIST Low security baseline.
• Any control enhancement we already have or institute is added as icing on the cake.
• The NIST process has been adapted to our needs. It does not literally follow everything in the NIST docs. Instead, it follows the NIST spirit of managing risk.
Aligning with NIST at IU

1. Inventory
2. Documentation
3. Risk Self-Assessment
4. Risk Response
5. Training
6. Oversight & Approval
7. Authority to Operate
8. Ongoing Risk Management
1. Inventory

- System details, ePHI location, security settings, BAAs, scan info, access methods, disposal information, etc.
- Software, version, patch level, BAAs, scan info, etc.
- Privileged access inventory - names, roles, dates authorized, etc.
- Incident log – incident summary, response.
## The Inventory

### System Inventory

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Dell PowerEdge XXXX</td>
<td>Avarelent/mymysql</td>
<td>Yes</td>
<td>No, vendor does not have access to the system</td>
<td>RHEL</td>
<td>6.4</td>
<td>Critical</td>
<td>ePHI</td>
<td>No</td>
<td>SFTP, HTTP, HTTPS</td>
<td>Yes</td>
<td>Active Directory, kerberos</td>
<td>80, 22, 443</td>
<td>80, 443</td>
<td>22, 80, 443</td>
<td>1/1/2014, Clean</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Software Inventory

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;System&gt;</td>
<td>Apache HTTPD</td>
<td>2.4</td>
<td>N</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
<td>AD</td>
</tr>
<tr>
<td></td>
<td>MySQL</td>
<td>5.8</td>
<td>N</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
<td>AD</td>
</tr>
<tr>
<td></td>
<td>Perl</td>
<td>8.4.1</td>
<td>N</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
<td>AD</td>
</tr>
<tr>
<td></td>
<td>Java</td>
<td>7.1</td>
<td>N</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
<td>AD</td>
</tr>
</tbody>
</table>

### Incident Log

<table>
<thead>
<tr>
<th>Name</th>
<th>Incident Date</th>
<th>Software Exploited</th>
<th>Incident Details</th>
<th>How Detected?</th>
<th>Date ISO Notified</th>
<th>How Responded?</th>
<th>ISO ATO Issued on</th>
</tr>
</thead>
</table>

### Privileged Access Inventory

<table>
<thead>
<tr>
<th>System</th>
<th>Name</th>
<th>Access Authorized</th>
<th>Type of Access</th>
<th>Access Terminated</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Name1</td>
<td>1/1/2010</td>
<td>System Administrator</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Name2</td>
<td>1/1/2010</td>
<td>System Administrator</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Name3</td>
<td>1/1/12</td>
<td>System Administrator</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Name4</td>
<td>1/1/12</td>
<td>System Administrator</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Name5</td>
<td>1/1/12</td>
<td>System Administrator</td>
<td></td>
</tr>
</tbody>
</table>

---

This document contains tables for system inventory, software inventory, incident log, and privileged access inventory. It is associated with University Information Technology Services and the NSF Cybersecurity Summit on 8/26/14.
2. Controls - The SSP

- We based our SSP on the templates used by DHHS, NASA, etc. use to satisfy FISMA.
- It specifies system name, categorization, contacts, purpose, diagram, component description, interconnections, boundaries, dependencies, and a complete catalog of NIST 800-53 security & privacy controls in place.
- Enterprise common controls addressing each NIST 800-53 control family are documented separately and referenced in the SSP.
The SSP

HIPAA “required” & “addressable” controls are color coded
The Enterprise Common Controls

FAMILY: ACCESS CONTROL

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control: The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   - An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   - Procedures to facilitate the implementation of the access control policy and associated access controls; and
2. Reviews and updates the current:
   - Access control policy [Assignment: organization-defined frequency]; and
   - Access control procedures [Assignment: organization-defined frequency].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

<table>
<thead>
<tr>
<th>P1</th>
<th>LO</th>
<th>AC-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>MO</td>
<td>AC-1</td>
<td></td>
</tr>
<tr>
<td>HIG</td>
<td>AC-1</td>
<td></td>
</tr>
</tbody>
</table>

The UIC’s university-wide IT policy administration process is described at: http://protect.iu.edu/cybersecurity/policies/process.

AC-2 ACCOUNT MANAGEMENT

Control: The organization:

1. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types];
Secure the documents

- Once you create compliance documentation, it becomes an asset that needs protecting.
- Secure documentation management is key.
- Centralizing documentation helps with this.
- Encrypting documents helps too.
- We require an NDA if an external entity (customer, vendor, etc.) wants to see our documents.
- HIPAA compliance document retention = 6 years.
3. The RA Report

- We do risk self-assessments.
- Managers & sys admins brainstorm and identify areas of vulnerabilities and risk for the system.
- The assessment documents risk areas, NIST controls that address those risks, residual vulnerabilities and risks, and risk severity.
- External, third party assessments are performed every five years.
# The RA Report

<table>
<thead>
<tr>
<th>Threat/Vuln. Pair #</th>
<th>Threat Event</th>
<th>Area of Exploitable Vulnerability</th>
<th>Risk Category</th>
<th>Risk Details</th>
<th>Mitigating NIST Controls</th>
<th>Mitigating NIST Controls/Factors Summary</th>
<th>Residual Vulnerability</th>
<th>Residual Risk Level</th>
<th>Risk Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Attack</td>
<td>Account management</td>
<td>Compromise of confidentiality and integrity, loss of accountability</td>
<td>Data exposure due to weak account management practices (account provisioning, locking, deprovisioning)</td>
<td>AC-2</td>
<td>Use of institutional accounts and mature account management practices.</td>
<td>Low</td>
<td>Mitigated by existing controls</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Attack</td>
<td>Password management</td>
<td>Compromise of confidentiality and integrity</td>
<td>Data exposure due to weak password management practices (password strength, expiration, password changes without validation, passwords in scripts)</td>
<td>IA-2, IA-4, IA-5, IA-6, IA-7</td>
<td>Use of institutional accounts and mature password management practices. No passwords in scripts.</td>
<td>Low</td>
<td>Mitigated by existing controls</td>
<td></td>
</tr>
</tbody>
</table>
| 3                  | Attack, reconnaissance | Logical access controls          | Compromise of confidentiality and integrity | Data exposure due to unauthorized access (firewall ports, generic accounts, accounts with no passwords, unsecured remote access) | AC-1, AC-3, AC-4, AC-6, IA-4, IA-7 | Most system components behind Data Center firewall. Generic accounts/accounts with blank passwords disabled. | (a) Application access to external data sources  
(b) <device> located outside Data Center firewall | (a) Moderate  
(b) Moderate | See POA&M |
| 4                  | Attack       | Privilege management              | Compromise of confidentiality and integrity | Data exposure due to unauthorized access resulting from weak privilege management (direct administrator account use, no explicit privilege authorization) | AC-1, AC-2, AC-3, AC-4, AC-13 | Explicit privilege authorization | No individual accountability due to administrative account | Moderate | See POA&M |
4. Response - POA&M

- Our Plan of Action & Milestones documents our response to the residual risks that are not addressed by the existing controls.
- The response includes things like whether the risk was accepted or transferred, reasons, time estimate and activities planned if mitigation is planned, etc.
- It is not possible always to respond to a risk due to budget, technology constraints, etc. We document this and try our best to address those using training or workarounds.
<table>
<thead>
<tr>
<th>Risk</th>
<th>Risk Level</th>
<th>Action</th>
<th>Milestone</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application access to external data sources</td>
<td>Moderate</td>
<td>Risk accepted pending evaluation. Risk will be calculated for each specific application installed and the nature of connection and addressed accordingly.</td>
<td>Each application connecting to an external source will be analyzed independently to evaluate and mitigate risk.</td>
<td></td>
</tr>
<tr>
<td>&lt;device&gt; located outside Data Center firewall</td>
<td>Moderate</td>
<td>Risk addressed. The volume of data has an adverse effect on the Data Center firewall and the end user experience. The risk is minimized through existing security controls that address the device specifically.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No individual accountability due to shared administrative accounts</td>
<td>Moderate</td>
<td>Risk addressed in the next column. The Citrix application requires the use of administrative accounts.</td>
<td>The risk will be mitigated via an access inventory of privileged access.</td>
<td>6/1/14</td>
</tr>
</tbody>
</table>
5. Staff Training

- **Annual training** is mandated for all who are involved in the care and feeding of the system (both management and staff).

- Three e-training modules must be completed:
  1. The standard IU HIPAA training (covering the reg and IU policies & procedures)
  2. IU Human Subjects training
  3. UITS specific information on how HIPAA applies to us, our policies & NIST procedures

- All security related is documented in a training log.
User Training

- All security measures at the back end can be defeated by security challenged users. They are typically the weakest link in the chain.
- We address this risk by providing guidance in our Knowledge Base about what is and is not permitted when handling ePHI on our systems.
- As we work individually with researchers, we train them & help them create HIPAA documentation that describes how they are protecting their end.
User awareness and training

What are my responsibilities when using UITS systems for work with electronic protected health information?

On this page:
- About ePHI and HIPAA compliance at IU
- About UITS HIPAA-aligned resources
- Your responsibilities when using UITS systems for work with ePHI
- Recommended technical safeguards
- Getting help

About ePHI and HIPAA compliance at IU

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) established rules protecting the privacy and security of personal health data. The HIPAA Security Rule set national standards specifically for the security of protected health information (PHI) that is created, stored, transmitted, or received electronically (i.e., electronic protected health information, or ePHI). To ensure the confidentiality, integrity, and...
6. Oversight

• When ready, the compliance package is sent to the IU HIPAA Privacy and Security Office, the University Information Security Office, and Internal Audit.

• We’d like every system under alignment to go through a full assessment but this is not done today due to (a) lack of resources, and (b) the trust that we have developed by working closely with these partners.

• Critical systems do get assessed.
7. Authority to Operate

• After we have reviewed everything and have approval from the partners, we issue an ATO.
• The ATO is good for thee years.
• Renewal requires a review of ongoing risk management practices, training, any incidents that may have occurred, response, etc.
• The ATO is a vehicle for a unit to self-assert compliance with oversight from us.
8. Ongoing Risk Management

- Once a system comes under alignment, it becomes subject to regular, ongoing risk management. This includes:
  - Semi-annual reviews, risk re-assessments, and documentation updates.
  - Continuous & automatic monitoring of risks, systems, generating alerts.
  - Annual training
  - Oversight
  - External assessments every five years
From NIST to HIPAA

- NIST 800-66 (An Introductory Resource Guide for Implementing the HIPAA Security Rule) provides HIPAA to NIST mapping.
- Our System Security Plan contains a HIPAA section that addresses HIPAA requirements that do not map to NIST.
- We will do the same for other rules and regulations such as IU’s critical data requirements, etc.
# NIST 800-66 HIPAA to NIST Crosswalk

## Table 4. HIPAA Standards and Implementation Specifications Catalog

|--------------------------------|--------------------------------|--------------------------------|------------------------------------------|-------------------------------|
| 164.308(a)(i)(i)               | Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations. | Risk Analysis (R): Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity. | RA-1 | FIPS 199  
NIST SP 800-14  
NIST SP 800-18  
NIST SP 800-30  
NIST SP 800-37  
NIST Draft SP 800-39  
NIST SP 800-42  
NIST SP 800-53  
NIST SP 800-53  
NIST SP 800-60  
NIST SP 800-84  
NIST SP 800-92  
NIST SP 800-100 |
| 164.308(a)(i)(ii)(A)           | Risk Management (R): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | Risk Management (R): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | RA-2, RA-3, RA-4, PL-6 | 
NIST SP 800-14  
NIST SP 800-18  
NIST SP 800-30  
NIST SP 800-37  
NIST Draft SP 800-39  
NIST SP 800-42  
NIST SP 800-53  
NIST SP 800-84  
NIST SP 800-92  
NIST SP 800-100 |
| 164.308(a)(i)(ii)(B)           | Sanction Policy (R): Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity. | Sanction Policy (R): Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity. | PS-8 | 
NIST SP 800-14  
NIST SP 800-18  
NIST SP 800-30  
NIST SP 800-37  
NIST SP 800-53  
NIST SP 800-84  
NIST SP 800-92  
NIST SP 800-100 |
| 164.308(a)(1)(ii)(C)           | Information System Activity Review (R): Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. | Information System Activity Review (R): Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. | AU-6, AU-7, CA-7, IR-3, IR-6, SI-4 | 
NIST SP 800-12  
NIST SP 800-14  
NIST SP 800-37  
NIST SP 800-53  
NIST SP 800-53A  
NIST SP 800-100 |
| 164.308(a)(2)                  | Assigned Security Responsibility: Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity. | Assigned Security Responsibility: Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity. | CA-4, CA-6 | 
NIST SP 800-12  
NIST SP 800-14  
NIST SP 800-37  
NIST SP 800-53  
NIST SP 800-53A  
NIST SP 800-100 |
IU SSP Section addressing HIPAA

4 HIPAA SAFEGUARDS NOT COVERED BY NIST 800-53 SECURITY AND PRIVACY CONTROLS

4.1 164.316(b)(2)(i) Time Limit
All compliance documentation is retained for six years as required by HIPAA.

4.2 164.316(b)(2)(ii) Availability
All documents are stored in the UITS Alfresco Share HIPAA aligned collaboration system. All UITS personnel that handle ePHI have accounts on this system and access to the documentation. The document owners are required to review the documentation semi-annually.
This shows how a NIST RMF provides an effective way to manage compliance.
Current Status

• At IU, we are establishing institutional processes for HIPAA/FISMA & IT compliance generally.
• HIPAA is in place for central HPC/IT.
• FISMA is in process.
• Like a lot of other places, the IU GRC (Governance, Risk, Compliance) framework is in flux and evolving. We are plugged into the thick of it due to effective partnerships.
Institutional HIPAA Process

1. Researcher needs HIPAA compliant IT solution
2. IU HIPAA Compliance Office, etc. sends them to us
3. We help build a HIPAA aligned solution
4. We help with documentation
5. Documentation is submitted to the ISO, Internal Audit, and HIPAA Compliance
6. The researcher self-asserts HIPAA compliance
Institutional FISMA Process*

1. Researcher gets/renews a govt. contract
2. Office of Research Admin (ORA) contacts us
3. We help build and monitor FISMA compliance
4. We help create a FISMA "package" for ORA
5. PI/ORA submit the package to agency
6. Agency issues an ATO

* = Future
Compliance is no beast

- The government does not expect you to undertake herculean measures or build walled gardens.
- Rules and regulations affecting cybersecurity are about using best practices, something we should be doing anyway.
- All of us have sufficiently good cybersecurity in place already. It won’t take a gargantuan effort to go all the way.
Future

• Expand the mature, standards-based NIST approach to all IT compliance at IU.
• Provide NIST-based risk and security assessment tools to all IT units for internal assessments.
• Centralize documentation which can be used by all units conducting IT assessments (UIISO, Internal Audit).
• Create/modify policies to be aligned with NIST.
Vision

• Establish an online risk profile system which automatically checks for new vulnerabilities, laws, etc. and provides alerts. We update the profile continuously as risks change.

• Institute central support for all IT related compliance.

We’d like to build compliance into the very fabric of our IT environment.
6. Conclusions
Compliance is Imminent

• Biomedical research is on a collision course with the HPC/research computing world.

• An increasingly larger volume of ePHI can be expected to land on academic HPC systems.

• Grants and contracts will be requiring FISMA ‘compliance’.

• It is coming, so embrace it.
Opportunities and Threats

- Not having a compliance process in place means missed opportunities, particularly for ‘Big Data’ applications in health sciences research.

- Managing ePHI without a RMF in place creates institutional liability and damage reputation.
Benefits

• A standards based RMF implementation aligns with other/future regulations, and can be part of an institutional risk management strategy.

• Customers with sensitive data will develop trust and bring new business.

• Your compliance folks will send people your way (ours do).

• You will better serve all your researchers.
You’re well on your way to compliance already!

• The government does not expect us to undertake herculean measures or build walled gardens.

• These regulations are about using best practices, something we should be doing anyway.

• All of us have sufficiently good information security in place already.
HIPAA/NIST Resources

- The HIPAA Security Rule

- NIST 800-66: Guide to Implementing the HIPAA Security Rule

- NIST 800-53: Recommended Security Controls


- NIST HIPAA Security Rule Toolkit

- IU NIST templates (email Anurag)
Contact

Anurag Shankar
ashankar@iu.edu

Bill Barnett
barnettw@iu.edu
License Terms


Items indicated with a © are under copyright and used here with permission. Such items may not be reused without permission from the holder of copyright except where license terms noted on a slide permit reuse.

Except where otherwise noted, contents of this presentation are copyright 2014 by the Trustees of Indiana University.

This document is released under the Creative Commons Attribution 3.0 Unported license (http://creativecommons.org/licenses/by/3.0/). This license includes the following terms: You are free to share – to copy, distribute and transmit the work and to remix – to adapt the work under the following conditions: attribution – you must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work). For any reuse or distribution, you must make clear to others the license terms of this work.