Aligning Your Research Cyberinfrastructure with HIPAA and FISMA

Anurag Shankar
Center for Applied Cybersecurity Research
Indiana University

2015 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure
August 17, 2015
## Schedule

<table>
<thead>
<tr>
<th>1. Introduction</th>
<th>1:00 – 1:05</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Research Cyberinfrastructure &amp; Compliance</td>
<td>1:05 – 1:15</td>
</tr>
<tr>
<td>3. A Gentle HIPAA Primer</td>
<td>1:15 – 1:45</td>
</tr>
<tr>
<td>4. A Gentler FISMA Primer</td>
<td>1:45 – 2:15</td>
</tr>
<tr>
<td>5. A Risk Management Primer</td>
<td>2:15 – 2:30</td>
</tr>
<tr>
<td>6. The NIST Risk Management Framework</td>
<td>2:30 – 3:00</td>
</tr>
<tr>
<td><strong>Break</strong></td>
<td><strong>3:00 – 3:30</strong></td>
</tr>
<tr>
<td>7. Building a Risk Management Framework</td>
<td>3:30 – 4:00</td>
</tr>
<tr>
<td>8. Using it to Address HIPAA &amp; FISMA</td>
<td>4:00 – 4:20</td>
</tr>
<tr>
<td>9. The Future</td>
<td>4:20 – 4:30</td>
</tr>
<tr>
<td>10. Conclusion, Q &amp; A / Discussion</td>
<td>4:30 – 5:00</td>
</tr>
</tbody>
</table>
1. Introduction
Quiz

• Do you know what kinds of data you have on your systems?

• Do you allow biomedical researchers on your systems?

• Have you a mechanism to stop sensitive data on the system?
Data Inventory

• A recent DLP exercise at IU showed that all 120 or so cloud storage systems are being used.

• Data flows showed plenty of personally identifiable health information.

• An Identity Finder run following a security incident on a user PC showed SSNs, etc.

* Big Data to Knowledge
Cybersecurity State of the Union

- Massive breaches this past year.
- On average half a million web attacks per day*. The network itself is being targeted now.
- Data exfiltration is most common, but new threats are emerging, in particular crypto-ransomware.
- Scary new targets (transportation, medical devices, etc.), IoT.

2015 Internet Security Threat Report, Symantec
Healthcare Cybercrime

• Healthcare is the most heavily targeted sector, breaches up 25%.

• Exfiltrated patient information being used for identity & insurance fraud, blackmail & extortion, celebrity snooping, etc.

• Patient records yield the highest price on the cybercrime market today.

• Problem as big as the data.
Weber, Mandl, and Kohane “Finding the Missing Link for Big Biomedical Data” JAMA 2014.4228
Where are we headed?

• Big Data spurring new areas of research, for instance electronic medical record (EMR) analytics, data repurposing, metadata harvesting, healthcare AI, etc.

• NIH calls this BD2K*.

• Coming to a … facility near you (campus, lab, NSF center??).

* Big Data to Knowledge
2. Research CI & Compliance
Major Cybersecurity Regulations Affecting Research

- Health Insurance Portability & Accountability Act (HIPAA) - 1996
- Federal Information Security Management Act (FISMA) – 2002
NIH

• Identifiable health data may be* subject to HIPAA Privacy.

• NIH funded researchers use a well established structure that handles HIPAA and FDA compliance (IRBs, Office of Research Administration, HIPAA Compliance Office, etc.)

• NIH is requiring FISMA compliance for contracts.

* HIPAA doesn't apply to all health data
NSF

• NSF doesn’t directly fund health research. However, it does fund social sciences and uses IRBs for human subjects research.

• Human subjects research must comply with the Common Rule*.

• FISMA may be coming to NSF contracts/grants.

Ready or Not …

• Analysis, storage, and management needs of health sciences research data reaching scales typical of physical sciences and engineering.

• Medical Center IT cannot keep pace.

• Existing local or national research CI often the only refuge.

• Health data ends up on our systems, often identifiable, without our knowledge or choice.
Challenges

• Researchers/CI providers are not regulatory experts.
• Cyber risk still a new concept for many.
• Lack of resources.
• Increasing HIPAA fines/audits.
• Potential loss of funding/face.
HIPAA & Research CI at Indiana University
Research CI at IU

- IU has had a mature, central research CI (local and national) for a couple decades now.
- CI provisioned through the Research Technologies (RT) division of the University Information Technology Services (UITS), IU’s central IT organization.
- RT delivers supercomputing, data storage/archival, visualization, application development & optimization, data management, etc.
HIPAA Intervenes

• Prior to 2000, IU’s central research CI used almost exclusively by the usual suspects - physical scientists and engineers.

• A Lilly Endowment grant to accelerate genomics research proposed using the existing CI for IU School of Medicine researchers.

• HIPAA compliance became a requirement.
It wasn’t until 2007 when HIPAA efforts to align our entire research CI began in earnest. The project took two years and required:

- Dedicated resources (1 FTE).
- Education (regulatory/security).
- An institution-wide committee for oversight and advocacy.
- An external gap and risk assessment.
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
HIPAA 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 controls 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
We received a blessing from the IU Compliance in 2009 of our “ability to handle ePHI”.

• … and starting from zero in 2009, we grew to:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></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>~1000</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>
Evolution

• Initial process and resources developed were largely homegrown & ad-hoc (much fumbling).
• Other rules/regulations such as FISMA, PCI-DSS, new IU IT risk policy, etc. were appearing on the horizon.
• By 2013 the structure was showing its age. It was also too HIPAA specific.
• A unified approach to compliance became apparent. (Most rules and regulations require risk management strategy and nearly the same controls.)
Compliance 2.0

• Needed a widely accepted standard.
• NIST chosen because it is a federal standard & addresses both HIPAA & FISMA compliance.
• It provides a persistent and evolving risk management framework, not just security controls.
• Strategy is to align with NIST first, then use mappings to specific regulations/requirements.
• Addresses departures from NIST explicitly.
Compliance 2.0 …

• The essential elements were there already.
• In 2013 added missing components - risk self assessment & mitigation, inventory, training, and more detailed documentation of controls.
• Documentation uses IU customized FISMA templates borrowed from DHHS/NASA.
• Transitioned to the new process over time, all new systems using it, old systems being migrated.
3. A Gentle HIPAA Primer
What is HIPAA?

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

• **Health Insurance Portability & Accountability Act.**
• Enforced by the Office for Civil Rights (OCR) in the US Dept. of Health & Human Services (DHHS).
• The HIPAA 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
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 protected
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 only applies to a covered entity (CE).
• Covered entities are healthcare providers, health plans, and health clearinghouses.
• Universities often choose to be hybrid covered entities, with both covered (healthcare) and non-covered components.
• HIPAA affects the whole CE. (For instance, the CE faces fines when a HIPAA violation occurs, not an individual department or employee.)
Am I covered?

- Your organization is not a covered entity if it is not involved in healthcare operations directly.
- You may still be subject to HIPAA if you serve a covered entity as a member of your covered entity’s workforce or as a Business Associate* and handle PHI for them in any way, shape, or form.
- You cannot say “I didn’t know we had PHI”.

* To be discussed
Business Associate

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.”

* BA is a HIPAA specific term
Business Associate Agreement

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

- You are not a BA if you are part of (say) a university providing services to its medical school.
- You are if you are (a) providing services to a CE completely separate from yours, and (b) store or process PHI for them.
- If the latter, the external CE must have a BAA with you (since your sys admins have access to user data).
- They are in violation of HIPAA if they do not.
What is a HIPAA Breach?

• An incident where an unauthorized disclosure of PHI has occurred.

• For instance a successful attack against a server which allows a hacker access to PHI, theft of an unencrypted device with PHI, loss of paper PHI, verbal disclosure, etc.

• Despite these situations, it may not be a breach if by forensics or other means you can show a high likelihood that no PHI was accessed.
A HIPAA Breach?

"Mrs. Cranley! You need to sign this HIPAA privacy form before the doctor can look at those warts on your stomach!"
Breach Notification

• HIPAA requires a breach of PHI to be reported to the OCR & patients whose data has been lost within 60 days.
• For breaches involving > 500 individuals, local media outlets must also be notified.
• Breaches are highly damaging.
• Not reporting a breach is a serious HIPAA violation that is liable for big penalties.
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 on or after 2/18/2009</td>
</tr>
<tr>
<td>Did Not Know (that a violation occurred)</td>
<td>Up to $100</td>
<td>$100 - $50,000</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>Up to $100</td>
<td>$1,000 - $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>
</tbody>
</table>
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, we are talking serious numbers here.
- Identity protection is universally expected after a beach. It’s not cheap!
HIPAA Civil/Criminal Penalties in Action

WellPoint to pay $1.7 million HIPAA penalty

Group slapped with $6.8M HIPAA fine

Another Big Fine After a Small Breach

Stanford reports fifth big HIPAA breach

On further review, $4.3 million Cignet HIPAA fine not a big surprise

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

$400,000 Penalty in HIPAA Case

$4.8M HIPAA Fine Part Of Wider HHS Crackdown

HHS attorney predicts big year for HIPAA fines

HIPAA Breaches in the Cloud

Tenet employee charged with theft, HIPAA violations

HIPAA Violation Indictments for 2 Medical Office Assistants

United States Attorney and L.S. Secret Service announced indictment of twelve individuals in a
Breaches reported by universities

**The absolute worst is being in the newspapers**
What happens after a breach?

• The OCR, affected individuals, and 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 the underlying risks.
• OCR may require a “Corrective Action Plan” and levy a fine.
• 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/implementation
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.

Courtesy Pointclear Solutions, Inc.
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 (e.g. HSO* required), 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

*HIPAA Security Officer
Required & Addressable

• Each Security Rule safeguard is either required or addressable.
  • Required = what it says.
  • Addressable = must 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 effort.
Standards and Implementation

- The Security Rule defines standards and 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.
Does HIPAA apply to all Identifiable Health Data?

- **No.** Only healthcare providers, facilities, and insurers are bound by HIPAA. Identifiable health data outside a healthcare context is not ePHI (though Common Rule still applies*).

- Data, if properly de-identified, is not subject to HIPAA.

If unsure, contact your HIPAA Compliance office!

* state rules may also apply
Who does HIPAA Cover at my organization?

• Employees, healthcare providers, trainees & volunteers at the medical school and affiliated healthcare sites or programs.
• Employees who work with university or organizational health plans.
• Employees who provide financial, legal, business, administrative, or IT support to the above.
Just Good Security?

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 environment.

- It requires a managed risk approach that proves due and ongoing diligence to OCR.

- Documentation is **key.** If it is not documented IN DETAIL, it doesn’t exist as far as OCR is concerned.
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 worked closely with our HIPAA Privacy and Security Officers. They are intimately engaged in our risk management process. They feel that we do sufficient due diligence and can survive a breach/audit.
HIPAA Myths

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

Sorry, none are true!
Here is what the DHHS says:

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

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

• There **IS** one way to be sure - an OCR audit! Due diligence is a lot easier.

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

- The HIPAA Security Rule allows you a lot of latitude depending on factors such as your size, budget, etc.
- This is both a boone and bane.
- It is highly open to local interpretation.
- Use your local HIPAA Compliance office to clarify what HIPAA means in your environment.
- If you don’t have such a unit, check with legal.
Breach Notification Stats as of 5/15: 500+ Breaches by Type

- Theft: 49%
- Unauthorized Access/Disclosure: 20%
- Loss: 9%
- Hacking/IT: 9%
- Other: 8%
- Improper Disposal: 4%
- Unknown: 1%

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

- Paper Records: 22%
- Desktop Computer: 12%
- Laptop: 20%
- Network Server: 13%
- Portable Electronic Device: 11%
- Email: 7%
- EMR: 4%
- Other: 11%

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 9%. However, even one breach 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 & media (laptops, USB sticks, phones).
• Paper records are still big.
Top Areas of Weakness Revealed by Breach Stats

- Risk Assessments
- Granting or Modifying Access
- User Activity Monitoring
- Authentication and Integrity
- Media Reuse and Destruction
- Contingency Planning
Most Common Causes of Citation from Recent OCR Audits

- No risk assessments
- Improper media movement and disposal
- No/inadequate audit controls and monitoring
4. A Gentler FISMA Primer
What is FISMA?

- Requires government agencies to secure their system as per NIST guidelines.
- The Office of the Inspector General does FISMA audits.
- There are also regular reporting requirements.
- Agency subcontractors (=you) also have to comply (similar to the HIPAA BA rule).
When does FISMA Apply?

• When your systems collect, process, store, transmit, or use govt. owned data on behalf of the agency as part of a contract, and possibly, grant.
• The contract or grant will explicitly state FISMA terms (L, M, or H).
• New FISMA language may be added to existing contracts.
• Most grants and contracts don’t involve FISMA.
DHHS Guidance

“FISMA's requirements follow agency information into any system which uses it or processes it on behalf of the agency. That is, when the ultimate responsibility and accountability for control of the information continues to reside with the agency, FISMA applies.”

- The term "on behalf of" indicates that only those entities that are acting, under agency principles, as agents, where DHHS (or a component) is the principal, are covered by FISMA.
FISMA

Define system boundaries
Assess Risk (NIST 800-30, 37, 39)
Apply Controls (NIST 800-53)
Evaluate Controls (NIST 800-53A)
Authority to Operate (ATO)
Define System Boundaries

• 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 logical collection of disparate components, etc.
• A conceptual boundary extends to all direct and indirect users of the system that receive output.
• Requires IT professionals to determine.
Assess Risk

• Guidance from NIST documents NIST 800-30, 37, and 39 is used to conduct a risk assessment.

• Individual risks and severity are identified.

• A prioritized list of risks by severity is created.
Apply Controls

• The NIST guidance document NIST 800-53 is used to select controls that mitigate risk.
• The contract specifies the required security baseline (High, Medium, or Low).
• This can be a significant undertaking, especially for FISMA High. There are over 800 controls to consider.
• Many organizations will not accept FISMA High contracts as a result.
Evaluate Controls

• Evaluation includes detailed, regular security assessments.
• Evaluation involves testing the controls in place to gauge their effectiveness in mitigating risk.
• Evaluations can be internal or external.
• The NIST 800-53A document covers evaluating NIST 800-53 controls.
Authority to Operate

- The information security plan, etc. is submitted to the government agency.
- An ATO letter is issued by the agency to the business owner (and some authoritative information security unit like the ISO) authorizing operations of the system.
- If remediation is required and is not too serious, the agency will issue an Interim Authority To Operate (IATO). The IATO will have a defined end date. The problems must be fixed by that date.
Plan of Action & Milestones

• The POA&M describes remediation steps.
• Even if a contractor receives an ATO, there still may be items for which the agency requires remediation. These weaknesses may not be significant enough to withhold an IATO/ATO, but they still must be corrected.
• Someone at your institution (the ISO?) must track these items and ensure that they are completed.
Academic FISMA Infrastructures

- IU does not have a formal FISMA process in place yet. We’re studying others.
- Of particular interest is Duke Medicine which has a relatively robust FISMA process.
- They have built an IaaS based, external FISMA hosting environment.
- Still, FISMA burdens are such that Duke won’t accept FISMA High contracts.
FISMA Requires Resources

• 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.

• They have PIs write in a FISMA line item in the budget.

• Be prepared to dedicate significant resources.
5. A Brief Risk Management Primer
Research Workflow & Compliance

Compliance in practice translates into protecting data end to end through its entire lifecycle, using sound risk management principles.

- **Pre-Grant**
  - Prelim. Investigation
  - IRB
  - CI Design

- **Proposal**
  - Proposal Prep
  - Budget
  - Proposal Funded

- **Execution**
  - Data Acquisition
  - Data Analysis
  - Simulation
  - Data Management
  - Data Sharing
  - Data Visualization
  - Data Publishing

- **Post-Grant**
  - Data Archival
  - Data Disposal

= may involve compliance
Managing Cybersecurity Risk

- Identify, assess, prioritize, and mitigate risk to information security, on an ongoing basis.
- Focuses on risk, not just plugging security holes willy nilly.

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

- 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 the beginning of the road in cyber risk management. You cannot manage risk without first figuring it out.

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

• Effort should be commensurate with budget, risk tolerance, and complexity.
Risk Management Framework

A mature RMF addresses risk holistically. It covers:

• Governance = institutional security organization, policies, sanctions, enforcement
• Risk management = assessment, mitigation through appropriate physical, administrative, technical controls, documentation
• Review = regular monitoring, reviews, reassessment, and mitigation
• Awareness and training
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
6. The NIST Risk Management Framework
The NIST RMF

- The FISMA slides earlier provide a taste of the NIST process to managing risk.
- Now we will take a detailed look at how the NIST RMF enables a comprehensive and yet flexible approach that adapts to any environment/scale.
- Translates into a security lifecycle.
- Steps are informed by NIST and other govt. guidance documents.
NIST Security Lifecycle
1. Categorize System

- 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</td>
<td>[44 USC, SEC. 3542]</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.</td>
<td>[44 USC, SEC. 3542]</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.</td>
<td>[44 USC, SEC. 3542]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
2. Select Controls

- FIPS 200 (Minimum Security Requirements for Federal Information and Information Systems) essentially points to NIST 800-53.

- NIST 800-53 (Security & Privacy Controls for Federal Information Systems and Organizations) provides a catalog of \( \sim 1000^{*} \) security controls. They are divided into control families with a baseline control and zero or more control enhancements (enhanced controls).

\[*\]

800-53 v4 has 240 baseline controls, 670 control enhancements, and 16 controls covering program management = 926 controls.
### Security Baselines

<table>
<thead>
<tr>
<th>Control</th>
<th>Security Baseline</th>
<th>Controls</th>
<th>Baseline Control</th>
<th>Security Baseline</th>
<th>Controls</th>
<th>Baseline Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-1</td>
<td>Access Control Policy and Procedures</td>
<td>P1</td>
<td>AC-1</td>
<td>AC-1</td>
<td>AC-1</td>
<td></td>
</tr>
<tr>
<td>AC-2</td>
<td>Account Management</td>
<td>P1</td>
<td>AC-2</td>
<td>AC-1 (1) (2) (3) (4)</td>
<td>AC-1 (1) (2) (3) (4)</td>
<td></td>
</tr>
<tr>
<td>AC-2</td>
<td>Account Management</td>
<td>P1</td>
<td>AC-2</td>
<td>AC-1 (1) (2) (3) (4)</td>
<td>AC-1 (1) (2) (3) (4)</td>
<td></td>
</tr>
<tr>
<td>AC-3</td>
<td>Access Enforcement</td>
<td>P1</td>
<td>AC-3</td>
<td>AC-3</td>
<td>AC-3</td>
<td></td>
</tr>
<tr>
<td>AC-4</td>
<td>Information Flow Enforcement</td>
<td>P1</td>
<td>AC-4</td>
<td>AC-4</td>
<td>AC-4</td>
<td></td>
</tr>
<tr>
<td>AC-5</td>
<td>Separation of Duties</td>
<td>P1</td>
<td>AC-5</td>
<td>AC-5</td>
<td>AC-5</td>
<td></td>
</tr>
<tr>
<td>AC-6</td>
<td>Least Privilege</td>
<td>P1</td>
<td>AC-6</td>
<td>AC-6 (1) (2) (3) (4)</td>
<td>AC-6 (1) (2) (3) (4)</td>
<td></td>
</tr>
<tr>
<td>AC-7</td>
<td>Unsuccessful Login Attempts</td>
<td>P1</td>
<td>AC-7</td>
<td>AC-7</td>
<td>AC-7</td>
<td></td>
</tr>
<tr>
<td>AC-8</td>
<td>System Use Notification</td>
<td>P1</td>
<td>AC-8</td>
<td>AC-8</td>
<td>AC-8</td>
<td></td>
</tr>
<tr>
<td>AC-9</td>
<td>Privileged Logon (Target) Notification</td>
<td>P1</td>
<td>AC-9</td>
<td>AC-9</td>
<td>AC-9</td>
<td></td>
</tr>
<tr>
<td>AC-10</td>
<td>Account Session Control</td>
<td>P1</td>
<td>AC-10</td>
<td>AC-10</td>
<td>AC-10</td>
<td></td>
</tr>
<tr>
<td>AC-11</td>
<td>Session Lock</td>
<td>P1</td>
<td>AC-11</td>
<td>AC-11</td>
<td>AC-11</td>
<td></td>
</tr>
<tr>
<td>AC-12</td>
<td>Session Termination</td>
<td>P1</td>
<td>AC-12</td>
<td>AC-12</td>
<td>AC-12</td>
<td></td>
</tr>
<tr>
<td>AC-13</td>
<td>Withdraw</td>
<td>P1</td>
<td>AC-13</td>
<td>AC-13</td>
<td>AC-13</td>
<td></td>
</tr>
<tr>
<td>AC-14</td>
<td>Permitted Actions without Identification or Authentication</td>
<td>P1</td>
<td>AC-14</td>
<td>AC-14</td>
<td>AC-14</td>
<td></td>
</tr>
<tr>
<td>AC-15</td>
<td>Withdraw</td>
<td>P1</td>
<td>AC-15</td>
<td>AC-15</td>
<td>AC-15</td>
<td></td>
</tr>
<tr>
<td>AC-16</td>
<td>Security Attributes</td>
<td>P1</td>
<td>AC-16</td>
<td>AC-16</td>
<td>AC-16</td>
<td></td>
</tr>
<tr>
<td>AC-17</td>
<td>Remote Access</td>
<td>P1</td>
<td>AC-17</td>
<td>AC-17 (1) (2) (3) (4)</td>
<td>AC-17 (1) (2) (3) (4)</td>
<td></td>
</tr>
<tr>
<td>AC-18</td>
<td>Wireless Access</td>
<td>P1</td>
<td>AC-18</td>
<td>AC-18</td>
<td>AC-18</td>
<td></td>
</tr>
<tr>
<td>AC-19</td>
<td>Access Control for Mobile Devices</td>
<td>P1</td>
<td>AC-19</td>
<td>AC-19</td>
<td>AC-19</td>
<td></td>
</tr>
<tr>
<td>AC-20</td>
<td>Use of External Information Systems</td>
<td>P1</td>
<td>AC-20</td>
<td>AC-20</td>
<td>AC-20</td>
<td></td>
</tr>
<tr>
<td>AC-21</td>
<td>Information Sharing</td>
<td>P1</td>
<td>AC-21</td>
<td>AC-21</td>
<td>AC-21</td>
<td></td>
</tr>
<tr>
<td>AC-22</td>
<td>Publicly Accessible Content</td>
<td>P1</td>
<td>AC-22</td>
<td>AC-22</td>
<td>AC-22</td>
<td></td>
</tr>
<tr>
<td>AC-23</td>
<td>Data Mining Problems</td>
<td>P1</td>
<td>AC-23</td>
<td>AC-23</td>
<td>AC-23</td>
<td></td>
</tr>
<tr>
<td>AC-25</td>
<td>Reference Monitor</td>
<td>P1</td>
<td>AC-25</td>
<td>AC-25</td>
<td>AC-25</td>
<td></td>
</tr>
<tr>
<td>AT-1</td>
<td>Security Awareness and Training Policy and Procedures</td>
<td>P1</td>
<td>AT-1</td>
<td>AT-1</td>
<td>AT-1</td>
<td></td>
</tr>
</tbody>
</table>

### Table D-2: Security Baseline Control Allocation

<table>
<thead>
<tr>
<th>CNTL NO.</th>
<th>CONTROL NAME</th>
<th>INITIAL CONTROL ALLOCATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-1</td>
<td>Access Control Policy and Procedures</td>
<td>P1 AC-1 AC-1 AC-1</td>
</tr>
<tr>
<td>AC-2</td>
<td>Account Management</td>
<td>P1 AC-2 AC-1 (1) (2) (3) (4) AC-1 (1) (2) (3) (4)</td>
</tr>
<tr>
<td>AC-3</td>
<td>Access Enforcement</td>
<td>P1 AC-3 AC-3 AC-3</td>
</tr>
<tr>
<td>AC-4</td>
<td>Information Flow Enforcement</td>
<td>P1 Not Selected AC-4 AC-4</td>
</tr>
<tr>
<td>AC-5</td>
<td>Separation of Duties</td>
<td>P1 Not Selected AC-5 AC-5</td>
</tr>
<tr>
<td>AC-6</td>
<td>Least Privilege</td>
<td>P1 Not Selected AC-6 (1) (2) (3) (4) AC-6 (1) (2) (3) (4)</td>
</tr>
<tr>
<td>AC-7</td>
<td>Unsuccessful Login Attempts</td>
<td>P1 Not Selected AC-7 AC-7</td>
</tr>
<tr>
<td>AC-8</td>
<td>System Use Notification</td>
<td>P1 AC-8 AC-8 AC-8</td>
</tr>
<tr>
<td>AC-9</td>
<td>Privileged Logon (Target) Notification</td>
<td>P1 Not Selected Not Selected Not Selected</td>
</tr>
<tr>
<td>AC-10</td>
<td>Account Session Control</td>
<td>P1 Not Selected Not Selected Not Selected AC-10</td>
</tr>
<tr>
<td>AC-11</td>
<td>Session Lock</td>
<td>P1 Not Selected AC-11 (1) AC-11 (1)</td>
</tr>
<tr>
<td>AC-12</td>
<td>Session Termination</td>
<td>P1 Not Selected Not Selected Not Selected AC-12 AC-12</td>
</tr>
<tr>
<td>AC-13</td>
<td>Withdraw</td>
<td>P1 Not Selected AC-13 AC-13 AC-13</td>
</tr>
<tr>
<td>AC-14</td>
<td>Permitted Actions without Identification or Authentication</td>
<td>P1 AC-14 AC-14 AC-14</td>
</tr>
<tr>
<td>AC-15</td>
<td>Withdraw</td>
<td>P1 Not Selected Not Selected Not Selected AC-15 AC-15</td>
</tr>
<tr>
<td>AC-16</td>
<td>Security Attributes</td>
<td>P1 Not Selected Not Selected Not Selected AC-16 AC-16</td>
</tr>
<tr>
<td>AC-17</td>
<td>Remote Access</td>
<td>P1 AC-17 (1) (2) (3) (4) AC-17 (1) (2) (3) (4)</td>
</tr>
<tr>
<td>AC-18</td>
<td>Wireless Access</td>
<td>P1 AC-18 AC-18</td>
</tr>
<tr>
<td>AC-19</td>
<td>Access Control for Mobile Devices</td>
<td>P1 AC-19 AC-19</td>
</tr>
<tr>
<td>AC-20</td>
<td>Use of External Information Systems</td>
<td>P1 AC-20 AC-20</td>
</tr>
<tr>
<td>AC-21</td>
<td>Information Sharing</td>
<td>P1 Not Selected AC-21 AC-21</td>
</tr>
<tr>
<td>AC-22</td>
<td>Publicly Accessible Content</td>
<td>P1 AC-22 AC-22</td>
</tr>
<tr>
<td>AC-23</td>
<td>Data Mining Problems</td>
<td>P1 Not Selected Not Selected Not Selected AC-23 AC-23</td>
</tr>
<tr>
<td>AC-24</td>
<td>Access Control Decisions</td>
<td>P1 Not Selected Not Selected Not Selected AC-24 AC-24</td>
</tr>
<tr>
<td>AC-25</td>
<td>Reference Monitor</td>
<td>P1 Not Selected Not Selected Not Selected AC-25 AC-25</td>
</tr>
<tr>
<td>AT-1</td>
<td>Security Awareness and Training Policy and Procedures</td>
<td>P1 AT-1 AT-1 AT-1</td>
</tr>
</tbody>
</table>

---

**Notes:**

- The security control baselines in Table D-2 are the initial baselines assigned by organizations prior to conducting the baseline assessment described in Section 2.2. The control baselines and priority codes are only applicable to non-national security systems. Security control baselines for national security systems are included in CNSF Instruction 1259.

---

**References:**

- NIST Special Publications 800-12, 800-100
- Priority and Baseline Allocation
- AC-2 ACCOUNT MANAGEMENT
  - a. Identifies and selects the following types of information systems accounts to support organizational mission/business functions: [Assignment: organization-defined information systems account types]
  - b. Assigns account managers for information systems accounts;
  - c. Establishes conditions for group and role membership;
  - d. Specifies authorized users of the information system, group and role membership, and access authorizations (e.g., privileges) and other attributes (as required) for each account;
  - e. Requires approval by [Assignment: organization-defined personnel or role] for requests to create information system accounts;
  - f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];
  - g. Manages the use of, information system accounts;
Control Enhancements

1. Least Privilege | 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.

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

3. 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 actual machine; (ii) employing hardware and/or software domain separation mechanisms and/or implementing separate physical domains.

4. Least Privilege | Unprivileged 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 equipment of-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 as organizations retain the ability to control information.
Control Baselines

• If you are aligning with the “low” security baseline*, you choose just those controls that are in the “LOW” column.
• More and more controls get added as you move to “medium” and “high” baselines**.
• FISMA low, medium, and high requirements correspond to these L,M,H security baselines.

* = Does not correspond to low (bad) security
** = Not to be confused with the FIPS 199 low, medium, high categorization
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. The documentation (the RA report) describes the methodology used, areas of risk and vulnerabilities, and severity.

- Risk response is documented in a document called the Plan of Action & Milestones (POA&M). It documents whether the risk was accepted, mitigated, or transferred and outlines the timelines and actions for mitigation.
3. Supplement Controls

• Results of the risk assessment may indicate supplemental controls needed to mitigate risk.
• 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.
Document Controls

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

• Many 800-53 controls will already be in place (typically).
• You will need to implement supplemental/missing controls.
• Controls don’t have to be implemented all at once. All you need is an implementation plan and timeline and document it in the Plan of Action and Milestones.
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 details of the assessment, for instance regular penetration testing.
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 the previous figure in detail.

- Authorization is based upon the information in the authorization package, namely the POA&M, the SSP, and the RA report.
7. Monitor 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.
7. Building a Risk Management Framework
Choosing a RMF

- You can choose from any number of RMFs available today.
- FAIR is a good one at modest scales.
- OCTAVE makes you sit down, brainstorm, and figure out risk.
- NIST is good for HIPAA and mandated for FISMA.
- We chose NIST because it’s a standard. Most any rule/regulation can be mapped to it.
Building a RMF at IU

• We chose NIST.
• We wanted to create a standards based foundation capable of handling all cyber compliance at IU (ultimately).
• It is in use now to align with HIPAA.
Design Goals

• Should be
  • lightweight and nimble
  • easily extensible to FISMA, etc.
  • reusable
  • doable (within budget, other constraints)
  • able to leverage pre-existing structure

• ??.
Pre-existing Structure

- Resources
  - Staff
  - HIPAA tools & expertise

- Processes
  - Workflows
  - Oversight

- Relationships
  - Compliance Office
  - IT units
Implementation Steps

1. Assign Resources
2. Develop tools
3. Develop process
4. Apply process to new systems
5. Migrate existing systems to new process
1. Assign Resources

- The project took about a year and 1 FTE.
- We align with the NIST “low” security baseline but also document pre-existing control enhancements.
2. Develop Tools

• We do not use the NIST process literally. We have adapted it to meet our goals & needs.
• The project took about a year and 1 FTE.
• We align with the NIST “low” security baseline but also document pre-existing control enhancements.
3. Develop Process

1. Inventory
2. Documentation of System & Controls
3. Risk Assessment
4. Risk Response
5. Awareness & Training
6. Oversight & Approval
7. Authority to Operate
8. Ongoing Risk Management

Center for Applied Cybersecurity Research
NSF Cybersecurity Summit 2015

INDIANA UNIVERSITY
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.
<table>
<thead>
<tr>
<th>System Inventory</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System</strong></td>
</tr>
<tr>
<td>system1.uts.iu.edu</td>
</tr>
<tr>
<td>system2.uts.iu.edu</td>
</tr>
</tbody>
</table>

The Inventory
Documentation of System & Controls

• Controls are documented in the “System Security Plan” or SSP.
• Template based on what DHHS, NASA, etc. use to satisfy FISMA.
• Describes system name, categorization, contacts, purpose, components, interconnections, boundaries, dependencies, and all NIST 800-53 security & privacy controls in place.
1.7 General Description / Purpose

The system name is a 77-digit alphanumeric code that identifies the system. It is used to uniquely identify the system in the organization's IT asset management system.

1.8 System Environment

The system environment is the set of hardware and software components that support the system. It includes the server hardware, the operating system, and the applications that run on the system.

2 NIST 800-53 SECURITY CONTROLS

2.1 (AC) Access Control

2.1.1 (AC-1) Access Control Policy and Procedures – L, N, H

The access control policy and procedures should be documented and maintained. The policy should include the following:

- Access control policy and procedures
- Access control mechanisms
- Access control decision
- Access control enforcement
- Access control monitoring and review
- Access control evaluation
- Access control disposition
- Access control documentation
- Access control training
- Access control audits

2.1.2 (AC-2) Account Management – L, M, H

The following account management policies should be documented and maintained:

- Account creation
- Account management
- Account expiration
- Account suspension
- Account deletion

2.1.3 (AC-3) Access Enforcement – L, M, H

The access enforcement policy and procedures should be documented and maintained. The policy should include the following:

- Access enforcement policy
- Access enforcement mechanisms
- Access enforcement decision
- Access enforcement enforcement
- Access enforcement monitoring and review
- Access enforcement evaluation
- Access enforcement disposition
- Access enforcement documentation
- Access enforcement training
- Access enforcement audits

2.1.4 (AC-4) Information Flow Enforcement

The information flow enforcement policy and procedures should be documented and maintained. The policy should include the following:

- Information flow enforcement policy
- Information flow enforcement mechanisms
- Information flow enforcement decision
- Information flow enforcement enforcement
- Information flow enforcement monitoring and review
- Information flow enforcement evaluation
- Information flow enforcement disposition
- Information flow enforcement documentation
- Information flow enforcement training
- Information flow enforcement audits

2.1.5 (AC-5) Separation of Duties – L, M, H

The following separation of duties policies should be documented and maintained:

- Separation of duties policy
- Separation of duties mechanisms
- Separation of duties decision
- Separation of duties enforcement
- Separation of duties monitoring and review
- Separation of duties evaluation
- Separation of duties disposition
- Separation of duties documentation
- Separation of duties training
- Separation of duties audits

2.1.6 (AC-6) Least Privilege – M (10/2018)

The least privilege policy and procedures should be documented and maintained. The policy should include the following:

- Least privilege policy
- Least privilege mechanisms
- Least privilege decision
- Least privilege enforcement
- Least privilege monitoring and review
- Least privilege evaluation
- Least privilege disposition
- Least privilege documentation
- Least privilege training
- Least privilege audits

2.1.7 (AC-7) Unauthorized Login Attemps

The unauthorized login attempts policy and procedures should be documented and maintained. The policy should include the following:

- Unauthorized login attempts policy
- Unauthorized login attempts mechanisms
- Unauthorized login attempts decision
- Unauthorized login attempts enforcement
- Unauthorized login attempts monitoring and review
- Unauthorized login attempts evaluation
- Unauthorized login attempts disposition
- Unauthorized login attempts documentation
- Unauthorized login attempts training
- Unauthorized login attempts audits

2.1.8 (AC-8) System Use Noticitation – L, M, H

The system use notice policy and procedures should be documented and maintained. The policy should include the following:

- System use notice policy
- System use notice mechanisms
- System use notice decision
- System use notice enforcement
- System use notice monitoring and review
- System use notice evaluation
- System use notice disposition
- System use notice documentation
- System use notice training
- System use notice audits

1.8.1 Information Flow

Describe how the data flows in a diagram to ensure no one data is at risk. Each flow is unique. It uses a username as an identifier.

1.8.1.1 Institutional Accounts

- <systemname> uses IUS Identity for authentication for the system.
- IUS Identity credentials are sufficient for the system.

1.8.1.2 Other Accounts

- Non-IUS accounts are not used for authentication.
- Other accounts are used for administrative purposes.

1.8.1.3 Exception

- Any exceptions to the above rules should be documented and maintained.
Enterprise Common Controls

- Individual SSPs describe hundreds of controls.
- A large number of these are inherited from the organization. They apply to all systems (enterprise common controls).
- It is wasteful to include them every time in each SSP.
- So enterprise common controls (ECC) are documented separately.
- Individual SSPs simply point to the ECC docs where needed.
The ECC Document
Risk Assessment

- External, third party (expensive!) assessments every few years.
- The unit does internal risk self-assessments (RSA).
- Managers & sys admins brainstorm and identify areas of vulnerabilities and risk for the system.
- The **RSA report** documents risk areas, controls that address those risks, residual vulnerabilities and risks, and risk severity.
# The RSA 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 Control/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, lack 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>
<tr>
<td>3</td>
<td>Attack, recon</td>
<td>Logical access controls</td>
<td>Compromise of confidentiality and integrity</td>
<td>Data exposure due to unauthorized access (firewall ports, generic accounts, accounts with no passwords, unsecured remote access)</td>
<td>AC-3, AC-5, AC-6, IA-2, IA-4, IA-5, IA-4, SC-7</td>
<td>Most system components behind Data Center firewall. Generic accounts/accounts with blank passwords disabled.</td>
<td>(a) Application access to external data sources (b) &lt;device&gt; located outside Data Center firewall</td>
<td>(a) Moderate (b) Moderate</td>
<td>See POA&amp;M</td>
</tr>
<tr>
<td>4</td>
<td>Attack</td>
<td>Privilege management</td>
<td>Compromise of confidentiality and</td>
<td>Data exposure due to unauthorized access resulting from weak privilege mismanagement (direct administrator account use, no</td>
<td>AC-1, AC-2, AC-3, AC-4, AC-5, AC-6, AC-7</td>
<td>Explicit privilege authorization</td>
<td>Moderate</td>
<td>See POA&amp;M</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** This table provides a summary of potential threats and vulnerabilities, along with recommendations for mitigating these risks. The controls listed are based on the NIST framework, and the response actions are designed to reduce the residual risk to an acceptable level.
Risk Response

• A “Plan of Action & Milestones” or POA&M documents the response to residual risks not addressed by existing controls.

• It states whether the risk was accepted, transferred, addressed, or to be mitigated, and reasons, timelines and planned mitigation activities/controls.

• Valid reasons for accepting a risk is budget, resource constraints, etc. We try our best to address them, for instance through training.
<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>8/1/14</td>
</tr>
</tbody>
</table>
Staff Training

- Annual training is mandated for both management and staff responsible for operating the system.
- Three e-training modules must be completed:
  1. The standard IU HIPAA training (covering the law and IU policies & procedures)
  2. IU Human Subjects training
  3. UITS specific information on how HIPAA applies to the IT organization specifically, our policies & NIST procedures
- All security related is documented in a training log.
User Training

• We provide online training and awareness via our Knowledge Base, YouTube videos, local media, in person classes, and email alerts.
• We recently (really) raised awareness by launching our own phishing attack.
• Fortunately, big breaches are having some effect.
• As we work individually with researchers, we train them as we help them create their own (HIPAA) documentation describing how they are protecting their end.
Oversight

• The complete compliance documentation package is sent to the IU HIPAA Privacy and Security Office, the University Information Security Office, and Internal Audit.

• They only do a light review presently due to lack of resources. This will hopefully change soon.

• High impact systems and those that have had major incidents do get a more thorough review.
Authority to Operate

• There is not a formal ATO process in place today.
• Alignment is essentially self asserted (with oversight as stated earlier).
• No one is willing to sign on a dotted line accepting risk for the institution (this is very typical of most institutions).
• For FISMA, all this will need to change.
Ongoing Risk Management

• Once a system comes under alignment, it becomes subject to regular, ongoing risk management until decommissioning. We require:
  • Semi-annual reviews, risk re-assessments, and documentation updates.
  • Continuous, automatic monitoring of systems.
  • Annual training.
  • Oversight.
  • External assessments.
4. Apply Process to New Systems

• Having started in 2007, most of our systems had gone through the old, non-NIST process.
• New systems needing alignments were naturally suited to the new process.
• While we worked on the NIST process, more and more ePHI began landing on our systems.
• Luckily, we were ready.
• To date, around 5 systems have gone through the new process.
5. Migrate Existing Systems

• Around 30 systems had gone through the old process.
• We are just starting to migrate these systems to the new process.
• Migration involves gutting the old documentation, salvaging what we can from it for the new, and adding the risk self-assessment/response piece.
• We expect it will take at least a year to finish the migration.
8. Using the RMF to Address HIPAA and FISMA
RMF to Compliance

• The RMF by itself does not give you compliance … but it makes complying a lot easier.

• Building the RMF is a demanding but one time exercise. Compliance is an ongoing activity as new systems are aligned.

• Having the RMF allows you to concentrate on the system being aligned and not worry about common dependencies, etc.

• It gives you confidence in your ability to comply.
The IU Approach

• Align all systems with NIST first, not individual regulations.
• Map the regulation to NIST. Such mappings already exist, for instance for HIPAA.
• We can do the same for other rules and regulations such as IU’s critical data requirements.
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 can do the same for other rules and regulations such as IU’s critical data requirements.
# NIST 800-66 HIPAA to NIST Map

## Table 4. HIPAA Standards and Implementation Specifications Catalog

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>164.308(a)(1)(i)</td>
<td>Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations.</td>
<td></td>
<td>RA-1</td>
<td>FIPS 199</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
<td>RA-2, RA-3, RA-4</td>
<td>NIST SP 800-14</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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)</td>
<td>RA-2, RA-3, RA-4, PL-6</td>
<td>NIST SP 800-18</td>
</tr>
<tr>
<td></td>
<td>Sanction Policy (R): Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.</td>
<td></td>
<td>PS-8</td>
<td>NIST SP 800-30</td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
<td>AU-6, AU-7, CA-7, IR-5, IR-6, SI-4</td>
<td>NIST SP 800-37</td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
<td>CA-4, CA-6</td>
<td>NIST SP 800-42</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-84</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-92</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-100</td>
</tr>
</tbody>
</table>
IU SSP Section Addressing HIPAA

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

4.1 164.308(b)(1) Business Associate Contracts and Other Arrangement
IU has a BAA with Forte Research Systems.

4.2 164.316(b)(2)(i) Time Limit
All compliance documentation is retained for six years as required by HIPAA.

4.3 164.316(b)(2)(ii) Availability
All documents are stored in Box. 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.
1. Researcher needs a HIPAA compliant IT solution
2. IU HIPAA Compliance Office, etc. sends them to us/They come to us
3. We help build a HIPAA aligned solution and/or provide consulting
4. We help with documentation
5. Documentation is submitted to the ISO, Internal Audit, and HIPAA Compliance
HIPAA Process for IT Units

1. IT unit needs to align an existing or new system
2. They come to us for help
3. We work with them 1:1 to create the compliance package
4. We mediate between them and the authorities during review
5. We help them with ongoing risk management
FISMA for Agencies

- FISMA = NIST + Accreditation + ATO + Reporting.
- Accreditation:
  - Security certification
  - Submission of documentation (SSP, RA, POA&M)
- ATO or interim ATO by the agency.
- Reporting:
  - SSP update
  - POA&M update
  - Status of continuous monitoring activities - vulnerabilities discovered, security impact analysis, security control monitoring
FISMA in Academia

• Starts with FISMA language in a grant/contract.
• Triggers a local administrative process.
• Requires the NIST RMF/documentation.
• The local administrative unit submits FISMA paperwork to the agency.
• The agency responds. An iATO may be issued.
• Remediation and more paperwork is then required.
• The final result is an ATO by the agency.
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
  - Clearly describe data flows
  - In detail, describe all systems used for contract work
However, a PI may be able to negotiate things down to something agreeable to the agency depending on factors such as the origin or sensitivity of the data, etc.
Institutional FISMA Process

1. Researcher gets/renews a govt. contract
2. Office of Research Admin (ORA) contacts us
3. Build and monitor FISMA compliance
4. Create a FISMA “package” for ORA
5. PI/ORA submit the package to agency
6. Agency issues an ATO
Outcomes

• At IU, NIST has allowed us to focus on a single standard and process for cyber compliance.
• We are beginning to establish an institutional structure for HIPAA/FISMA & other current and future regulations.
• Units engaged in compliance like the process.
• We feel confident in our ability to handle audits.
9. The Future
1. Cloud

- Cloud seriously complicates compliance.
- … but, many cloud vendors are now providing HIPAA “compliant” solutions and willing to sign a HIPAA BAA.
- This includes Amazon (AWS) and Microsoft (Azure). It’s possible to build compliant solutions.
- IU just allowed ePHI on IU’s enterprise Box … but it required much due diligence and many local controls.
FedRAMP

• Federal Risk and Authorization Management Program for secure cloud certification.

• Cloud vendors must have a FedRAMP certification to comply with FISMA and thus be eligible for govt. contracts.

• Presumably, one can use a FedRAMP certified cloud solution to build a FISMA compliant solution. It’s unlikely to be cheap though.
2. Automation

- Automated inventory & configuration management systems, automated checks for existing/new vulnerabilities & changes in regulations, automated alerts, continuous monitoring for evolving risks, etc. (SANS top 20 is a good source for information.)

- Electronic governance, risk, and compliance (e-GRC) systems fed by a these which also manages BAAs, policies, audits, vendors, incidents, etc. (Examples of e-GRC systems includes RSA Archer, LockPath, Compliance 360, GRC Cloud, Modulo, Agiliance, Accelus, etc.)
3. Metrics Based Security?

- Cybersecurity today is mostly devoid of metrics or models that are useful.
- There is a desire to move to quantitative cybersecurity but it’s long ways away.
- SANS has done a great job with their top 20 controls. While not quantitative, they are based on actual attack metrics, not theoretical attacks.
- Most useful are their “low hanging fruits”, controls that can prevent a majority of the common attacks.
4. Evolution of Approach

- The internet started with little to no security.
- This was followed by security “best practices”.
- Cybersecurity standards such as ISO, NIST, etc. emerged.
- Existing risk management concepts were then borrowed from other areas.
- There is growing hopelessness and realization that the bottom line is to achieve the ability to function despite attacks/incidents.
“Cyber Resilience”

We can approach cybersecurity in human health terms:

- Diseases (successful cyber attacks) are inevitable.
- Prevention, detection, intervention (incident response, DR/BCP), monitoring & ongoing treatment (cyber risk management) are known to be effective in curing or containing disease.

- A major difference is the absence of cure!
- Change assumption from “if I have enough controls, all will be well” to “I will be hacked”.
- Approach the problem holistically, not piecemeal.
Fore more information, see US-CERT’s Cyber Resilience Review (CRR) site.

https://www.us-cert.gov/ccubedvp/self-service-crr

Cyber Resilience Review (CRR):
Method Description and Self-Assessment User Guide

February 2014
10. Conclusion
Compliance is Imminent

• Biomedical research is on a collision course with research CI.

• With little biomedical research CI around, an increasingly larger volume of ePHI can be expected to land on our systems.

• Grants and contracts will be asking for FISMA compliance.

• … So embrace it.
HIPAA/FISMA are Doable

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

• Rules and regulations affecting information security are about using best practices, something we should be doing anyway.

• Most of us have sufficiently good information security in place already. It won’t take a gargantuan effort to go all the way.
Opportunities and Threats

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

• … and therefore for funding.

• Managing ePHI without a RMF in place makes life hard and creates a potential for institutional liability and reputational damage.
Benefits

- A standards based RMF implementation makes you rule/regulation proof.
- Customers with sensitive data will trust your shop, bringing new business.
- Your compliance folks will send people your way (ours do).
- You will better serve researchers/your mission.
Questions/Discussion
Links

- 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
- NIST Templates (email me)
Interesting Reading

- “FISMA Continues to Challenge”: http://fcw.com/articles/2012/03/14/federal-agencies-fisma-compliance.aspx
Contact

Anurag Shankar
ashankar@iu.edu