University of Pittsburgh

Regulations and Compliance for Security and Researchers

Joel Garmon
Chief Information Security Officer
Joel.Garmon@pitt.edu
412-624-5595

June 14, 2018

Agenda

- Overview of Regulations
- Background of NIST 800-171
- Why it matters
- Controls
- Questions

HIPAA Security

- Health Insurance Portability and Accountability Act (HIPAA)
  - 18 primary requirements
  - 42 secondary requirements
  - Lots of nuances and guidance from HHS auditors

HIPAA Security Requirements

- **Administrative Safeguards**
- Security Management Process
- Assigned Security Responsibility Security
- Workforce security
- Information access management
- Security awareness and training
- Password management
- Security incident procedures
- Contingency plan
- Business associate contracts and other

- **Physical Safeguards**
- Facility access controls
- Workstation security
- Device and media

- **Technical Safeguards**
- Access control
- Audit controls
- Integrity
- Person or entity
- Transmission security Encryption

HIPAA Identifiers

1. Names;
2. All geographical subdivisions smaller than a State,
3. All elements of dates (except year) for dates directly related to an individual,
4. Phone 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; and
18. Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code the data)

Federal Drug Administration Trials

- Title 21 CFR Part 11-- Electronic Records; Electronic Signatures
  - maintain the records or submit designated information electronically and, as a result, have become subject to part 11

- https://www.fda.gov/RegulatoryInformation/Guidances/ucm125067.htm

Other Regulations or Contracts

- Personally Identifiable Information (PII)
  - Social security number
  - Passport information
  - Bank information
  - Tax returns and financial information
  - Other ID theft information
- Gramm-Leach-Bliley Act (GLB)
- Credit card information
- Research grants or contracts

Background of NIST 800-171

National Institute of Standards and Technology (NIST) 800-171

- **Title:** Protecting **Controlled Unclassified Information** in Nonfederal Information Systems and Organizations
- **Purpose:** Establishes an open and **uniform** program for managing information that that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, excluding information that is classified under Executive Order 13526 of December 29, 2009, or the Atomic Energy Act, as amended.

Why it matters

- Federal contracts may require compliance NIST 800-171
  - Review Office of Research contract language to determine if the IT environments must be NIST 800-171 compliant
    - Examples include:
      - Defense contracts include DFARS reference 252.204-7012 - Safeguarding Covered Defense Information and Cyber Incident Reporting
      - Contract terms state NIST 800-171 must be followed
      - Data is specifically identified as Controlled Unclassified Information (CUI)

Why it matters

- Department of Education dropping not-so-subtle hints it may be coming…

- "The Department strongly encourages institutions to review and understand the standards defined in the NIST SP 800-171, the recognized information security publication for protecting "Controlled Unclassified Information (CUI)," a subset of Federal data that includes unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Federal policies."
- "Thus, we strongly encourage those institutions that fall short of NIST standards to assess their current gaps and immediately begin to design and implement plans in order to close those gaps using the NIST standards as a model."

Dear Colleague Letter

July 1, 2016

DCL ID: GEN-16-12

Importance of Compliance

Controlled Unclassified Information (CUI)

- Any federal information that is not in the classified category
  - 22 approved CUI categories with 85 Subcategories

CUI Categories	
1. Agriculture	12. Law Enforcement
2. Copyright	13. Legal
3. Critical Infrastructure	14. NATO
4. Emergency Management	15. Nuclear
5. Export Control	16. Patent
6. Financial	17. Privacy
7. Foreign Government	18. Proprietary
8. Geodetic Product Information	19. Safety Act Information
9. Immigration	20. Statistical
10. Information Systems Vulnerability Information	21.Tax
11. Intelligence	22. Transportation

Subcategory Examples
Bank Secrecy
DNA
Investigation
Financial
Health Information
Personnel
Census
Investment Survey

https://csrc.nist.gov/csrc/media/projects/forum/documents/feb2014/pviscuso_cui-briefing.pdf

Achieving compliance

NIST 800-171 – High-level Controls

		Security Requirements	
#	CUI Security Requirements	Basic	Derived
3.1	Access Control	2	20
3.2	Awareness and Training	2	1
3.3	Audit and Accountability	2	7
3.4	Configuration Management	2	7
3.5	Identification and Authentication	2	9
3.6	Incident Response	2	1
3.7	Maintenance	2	4
3.8	Media Protection	3	6
3.9	Personnel Security	2	0
3.10	Physical Protection	2	4
3.11	Risk Assessment	1	2
3.12	Security Assessment	3	0
3.13	System and Communication Protection	2	14
3.14	System and Information Integrity	3	4

- 14 Security Requirement Families
- 109 Security Requirements
- Two types of Requirements
  - Basic
    - **What needs done**
    - Based on FIPS – 200
    - High-level security requirement
  - Derived
    - **How it can be done**
    - Based on NIST 800-53
    - Supplement the Basic requirements

NIST 800-171

- Required for many areas
- Becoming an industry ‘best practice’ even if not required
- Common standard for protecting information across the university or institution
  - If there is not requirement for a specific standard or review criteria, NIST 171 will meet most requirements for reviews

Other Security Standards or Frameworks

- NIST 800-53 and NIST Security Framework – government and general industry
  - https://nvd.nist.gov/800-53
  - https://www.nist.gov/cyberframework
- HITRUST – HIPAA
  - https://hitrustalliance.net/
- ISO 27000 series – international standards
  - 27001 ISO/IEC 27001 Information security management
  - 27002 Code of Practice for InfoSec Controls
  - 27017 Cloud Security Standards

References

- http://csrc.nist.gov/groups/SMA/forum/documents/feb2014/pviscuso_cui-briefing.pdf
- http://csrc.nist.gov/groups/SMA/forum/documents/aug-2016/tues400_sp800-171_dempsey.pdf
- https://library.educause.edu/~/media/files/library/2016/4/nist800.pdf
- http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf
- https://ifap.ed.gov/dpcletters/GEN1612.html

Questions???

Thank You