MANAGING COMPLIANCE
Title III of the E-Government Act (2002), entitled the Federal Information Security Management Act (FISMA) requires each federal agency to develop, document, and implement an agency-wide 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.

**WHAT IS FISMA?**

FISMA COMPLIANCE

- **PLAN FOR SECURITY**
  Understanding the procedure

- **SECURITY RESPONSIBILITY**
  Ensuring appropriate officials are assigned

- **SECURITY CONTROLS**
  Periodically reviewed in their information systems

- **AUTHORIZE SYSTEM PROCESSING**
  Prior to operations and, periodically, thereafter
FISMA SECURITY CERTIFICATION

17 families of control, over 180 controls, sub-controls

Lifecycle documentation: Security Plan, Risk Assessment Plan, Contingency Plan, Incident Response Plan, etc.

Yearly security assessments (including third party audits)

Change Management (Change Control Board)

Background checks of staff

Strict government oversight and notification
WHAT IS NIST’S ROLE?

NIST

Standards, guidelines, and other publications to assist federal agencies implement FISMA

SP 800-53


Catalog of security controls for all U.S. federal information systems except those related to national security
FISMA Certified Program
Hosting for the last 8 years

FISMA Certification
Compliance with NIST 800-53 requirements

Sponsoring Agency
Centers for Medicare & Medicaid Services (CMS), adds additional requirements through the CMS Acceptable Risk Safeguards (ARS)

Yearly Federal Audit
Required of 800-53 & CMS ARS Security Controls
HIPAA

**Title I:** Protects health insurance coverage for workers and their families when they change or lose their jobs

**Title II:** Administrative Simplification (AS) provisions—requires the establishment of national standards of electronic health care transactions and national identifiers for providers, health insurance plans, and employers.

---

**Privacy Rule (45 CFR part 160 and subparts A & E of part 164)**

- **ESTABLISH PRIVACY RIGHTS**
  For individual health information

- **STRUCTURED SANCTION POLICY**
  Required of covered entities to have in place

---

**Security Rule (45 CFR part 160 and subparts A & C of part 164)**

- **PROTECTED HEALTH INFORMATION**
  (PHI) - regulations for use and disclosure

- **REQUIRED SAFEGUARDS**
  Administrative, physical, and technical to ensure confidentiality, integrity and security of electronic PHI
SECURITY CONTROL REQUIREMENTS
HIPAA defines broad security control requirements
  • Language like “reasonably and appropriately” controls

MEETING STATED REQUIREMENTS
A challenge for HIPAA is to determine the most appropriate way to meet the stated requirements
  • Example HIPAA standard: “Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.”
Leveraged FISMA Experience
To guide interpretation of the most appropriate Security Controls

HIPAA Cloud
Hosted by SDSC for the last 4 years; built to NIST 800-53 specification

Audit/Assessment
Both external and internal

Multi-Tenant Cloud
For Researchers and business units requiring CUI & HIPAA compliance
Requirements to protect CUI are outlined in **NIST 800-171**

**NIST 800-171** requirements based on **NIST 800-53** Moderate baseline (and FIPS 200)

**NIST 800-171** applies to CUI when other laws/regulations are not applicable for protection (e.g. FISMA)

Requirements apply to:
- All components of nonfederal information systems
- Organizations that process, store or transmit CUI, or provide security protection for those components

Requires security protection when processed, stored, transmitted & used in nonfederal information systems
NARA defines what information qualifies as CUI in the CUI Registry (i.e., 22 top-level categories of data, with subcategories covering everything from electronic fund transfers to source selection in the procurement process)

CUI in Higher Education

- Student Records/PII
- Export control research data
- Critical infrastructure information
- Controlled technical information
EXAMPLE CUI CONTROLS

Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.

Ensure equipment removed for off-site maintenance is sanitized of any CUI.

Sanitize or destroy information system media containing CUI before disposal or release for reuse.

Cryptographic mechanisms to protect CUI confidentiality on transport; otherwise by physical safeguards.

Screen individuals prior to authorizing access to information systems containing CUI.
Organizations that are interested in or required to comply with the recommendations in this publication are strongly advised to review the complete listing of security controls in the moderate baseline in Appendix E to ensure that their individual security plans and security control deployments provide the necessary and sufficient protection to address the range of cyber and kinetic threats to organizational missions and business operations.
Nonfederal organizations describe in a system security plan (SSP), how the CUI requirements are met or how organizations plan to meet the requirements. The SSP describes the boundary of the information system; the operational environment for the system; how the security requirements are implemented; and the relationships with or connections to other systems. When requested, the SSP and any associated plans of action and milestones (POAM) for any planned implementations or mitigations should be submitted to the responsible federal agency or contracting officer to demonstrate the nonfederal organization’s implementation or planned implementation of the CUI requirements. Federal agencies may consider the submitted SSPs and POAMs as critical inputs to an overall risk management decision to process, store, or transmit CUI on an information system hosted by a nonfederal organization and whether or not to pursue an agreement or contract with the nonfederal organization.”
CYBERSECURITY FRAMEWORK (CSF)

NIST CSF provides a policy framework of computer security guidance for how organizations can assess and improve their ability to prevent, detect, and respond to cyber attacks.

It “provides a high level of taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes.”

GUIDANCE
On how to use an assessment of the business risks to guide their use of the framework in a cost-effective way.
Based on NIST Special Publication (SP) 800-30, Risk Management Guide for Information Technology Systems

RISKS REVIEWED YEARLY

Addresses the security controls that are specifically cited in the Cyber Security Framework

Documents the Risk Assessment approach that meets the CSF Risk Assessment requirements
<table>
<thead>
<tr>
<th></th>
<th>Example Sherlock Security Controls That Apply to HIPAA, CUI &amp; CSF</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>System Maintenance (timely patch/flaw redemption); <em>example</em>: 5 calendar days for critical rated vulnerabilities</td>
</tr>
<tr>
<td>2</td>
<td>Central Log collection and review of system logs</td>
</tr>
<tr>
<td>3</td>
<td>Intrusion Detection Systems (IDS) monitoring, review, analysis and reporting</td>
</tr>
<tr>
<td>4</td>
<td>Network Firewall Segmentation (defense in depth strategy)</td>
</tr>
<tr>
<td>5</td>
<td>Strong Authentication-2 factor using SecurID one-time tokens for privileged accounts</td>
</tr>
<tr>
<td>6</td>
<td>Protection of data-at-rest through encryption (FIPS 140-2)</td>
</tr>
<tr>
<td>7</td>
<td>Full backup/archive including offsite copy</td>
</tr>
<tr>
<td>8</td>
<td>Hardened system configurations (STIG and CIS)</td>
</tr>
</tbody>
</table>
### Example Sherlock Security Controls that Apply to HIPAA, CUI & CSF

<table>
<thead>
<tr>
<th>#</th>
<th>Security Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>Use of jump-boxes to isolate systems, limit system exposure</td>
</tr>
<tr>
<td>10</td>
<td>Encrypted tunnels for data-in-transit outside of private network (SSH, RDP, SSL)</td>
</tr>
<tr>
<td>11</td>
<td>Web Proxies and filters to limit web access</td>
</tr>
<tr>
<td>12</td>
<td>Limit use of email (block outbound email)</td>
</tr>
<tr>
<td>13</td>
<td>Data Use Agreements signed prior to access to systems/data, Data identification &amp; documentation</td>
</tr>
<tr>
<td>14</td>
<td>Host based firewalls</td>
</tr>
<tr>
<td>15</td>
<td>Secure data upload tool, encrypted tunnel to external systems</td>
</tr>
<tr>
<td>16</td>
<td>Malicious software protection (Anti-Virus/Malware SW)</td>
</tr>
</tbody>
</table>
To learn more about how we can put the Sherlock Cloud to work for you, visit our website at:

sherlock.sdsc.edu

Or

Email us at:

sherlock@sdsc.edu