CONTACT US

**Pylon Technology**
136 Main Street  Westport, CT  06880
W: www.pylontechnology.com
E: info@pylontechnology.com
T: +1 203 930 3410

PYLON TECHNOLOGY
Your Technology Advisor

# HIPAA ASSESSMENT GUIDELINES

Tim Quinn
CTO, Pylon Technology

WHITEPAPER
07/09/2017

pylontechnology.com info@pylontechnology.com +1 203 930 3410

# ABOUT **US**

With over 50 years combined experience from the management team alone, Pylon's story is a great one. Simply put, we've grown organically with our clients year over year.

## OUR **PROFILE**

*Pylon Technology is a Connecticut-based technology advisory firm. We specialize in helping you achieve your business goals by using technology to advance your own business goals and driving bottom-line through efficiency and simplicity.*

## WHAT **WE DO**

- Technology strategy & planning
- Managing business infrastructure
- Cybersecurity and compliance advisory
- Expense Control Management

Pylon Technology distinguishes itself by standing shoulder-to-shoulder with each client, as outsourced IT partners, while considering your company's business model, we take into consideration its mission, existing technology, and business goals. This information is then utilized to form a comprehensive IT long-term strategy. We provide clear and coherent options, along with extensive cost/benefit analyses, empowering you to make informed decisions.

We provide true advocacy computer consulting, implementation services, and support. At the core of our industry-leading client retention is establishing and maintaining our role as your trusted technology advisor.

# HIPAA OVERVIEW

The HIPAA Security Rule was the first attempt at a nationwide security standard for the protection of electronic protected health information (ePHI). The main goal of the HIPAA Security Rule is to implement the proper safeguards to protect the confidentiality, integrity, and accessibility (CIA) of ePHI. The second goal is to protect patient information while allowing the health care industry to expand and utilize technology to advance care delivery. Theree are 4 distinct parts to the Security Rule:

## ADMINISTRATIVE SAFEGUARDS

Administrat ve Safeguards are a specia subset of the HIPAA Security Rule that focus on internal organization, policies, procedures, and maintenance of security measures that protect patient health information.

## PHYSICAL SAFEGUARDS

As stated in the HIPAA Security Series, physical safeguards are "physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion."

## TECHNICAL SAFEGUARDS

According to the HIPAA Security Rule, technical safeguards are "the technology and the policy and procedures for its use that protect electronic protected health information and control access to it."

## ORGANIZATIONAL REQUIREMENTS

The majority of the HIPAA Security Rule consists of administrative, physical, and technical safeguards. The last four standards of the HIPAA Security Rule define administrative requirements to support the entirety of the Security Rule.

pylontechnology.com info@pylontechnology.com +1 203 930 3410

# HIPAA STANDARDS

| Administrative Safeguards | HIPAA Citation |
|---|---|
| **Security Management Process** | **164.308(a)(1)(i)** |
| Risk Analysis: Conduct Vulnerability Assessment | **164.308(a)(1)(ii)(A))** |
| Risk Management | **164.308(a)(1)(ii)(B)** |
| Sanction Policy | **164.308(a)(1)(ii)(C)** |
| Information System Activity Review | **164.308(a)(1)(ii)(D)** |
| **Assigned Security Responsibility** | **164.308(a)(2)** |
| **Workforce Security** | **164.308(a)(3)(i)** |
| Authorization and/or Supervision | **164.308(a)(3)(ii)(A)** |
| Workforce Clearance Procedure | **164.308(a)(3)(ii)(B)** |
| Termination Procedures | **164.308(a)(3)(ii)(C)** |
| **Information Access Management** | **164.308(a)(4)(i)** |
| Isolation Health Clearinghouse Functions | **164.308(a)(4)(ii)(A)** |
| Access Authorization | **164.308(a)(4)(ii)(B)** |
| Access Establishment and Modification | **164.308(a)(4)(ii)(C)** |
| **Security Awareness Training** | **164.308(a)(5)(i)** |
| Security Reminders | **164.308(a)(5)(ii)(A)** |
| Protection from Malicious Software | **164.308(a)(5)(ii)(B)** |
| Log-in Monitoring | **164.308(a)(5)(ii)(C)** |
| Password Management | **164.308(a)(5)(ii)(D)** |
| **Security Incident Procedures** | **164.308(a)(6)(i)** |
| Response and Reporting | **164.308(a)(6)(ii)** |

| Administrative Safeguards (Continued) | HIPAA Citation |
|---|---|
| **Contingency Plan** | **164.308(a)(7)(i)** |
| Data Backup Plan | **164.308(a)(7)(ii)(A)** |
| Disaster Recovery Plan | **164.308(a)(7)(ii)(B)** |
| Emergency Mode Operation Plan | **164.308(a)(7)(ii)(C)** |
| Testing and Revision Procedures | **164.308(a)(7)(ii)(D)** |
| Applications and Data Criticality Analysis | **164.308(a)(7)(ii)(E)** |
| **Evaluation** | **164.308(a)(8)** |
| **Business Associate Contracts and Other Arrangements** | **164.308(b)(1)** |
| Written Contract | **164.308(b)(4)** |

pylontechnology.com info@pylontechnology.com +1 203 930 3410

| Physical Safeguards | HIPAA Citation |
|---|---|
| **Facility Access Controls** | **164.310(a)(1)** |
| Contingency Operations | **164.310(a)(2)(i)** |
| Facility Security Plan | **164.310(a)(2)(ii)** |
| Access Control Validation Procedures | **164.310(a)(2)(iii)** |
| Maintenance Records | **164.310(a)(2)(iv)** |
| **Workstation Use** | **164.310(b)** |
| **Workstation Security** | **164.310(c)** |
| **Device and Media Controls** | **164.310(d)(1)** |
| Disposal | **164.310(d)(2)(i)** |
| Media Re-use | **164.310(d)(2)(ii)** |
| Accountability | **164.310(d)(2)(iii)** |
| Data Backup and Storage | **164.310(d)(2)(iv)** |

| Technical Safeguards | HIPAA Citation |
|---|---|
| **Access Control** | **164.312(a)(1)** |
| Unique User Identification | **164.312(a)(2)(i)** |
| Emergency Access Procedure | **164.312(a)(2)(ii)** |
| Automatic Logoff | **164.312(a)(2)(iii)** |
| Encryption and Decryption | **164.312(a)(2)(iv)** |
| **Audit Controls** | **164.312(b)** |
| **Integrity** | **164.312(c)(1)** |
| Mechanism to Authenticate EPHI | **164.312(c)(2)** |
| **Person or Entity Authentication** | **164.312(d)** |
| **Transmission Security** | **164.312(e)(1)** |
| Integrity Controls | **164.312(e)(2)(i)** |
| Encryption | **164.312(e)(2)(ii)** |

pylontechnology.com info@pylontechnology.com +1 203 930 3410

| Organizational Requirements | HIPAA Citation |
|---|---|
| **Business Associate Contracts or Other Arrangements** | **164.314(a)(1)** |
| Business Associate Contracts | **164.314(a)(2)** |
| **Requirements for Group Health Plans** | **164.314(b)(1)** |
| Implement Safeguards | **164.314(b)(2)(i)** |
| Ensure Adequate Separation | **164.314(b)(2)(ii)** |
| Ensure Agents Safeguard | **164.314(b)(2)(iii)** |
| Report Security Incidents | **164.314(b)(2)(iv)** |
| **Policies and Procedures** | **164.316(a)** |
| Documentation | **164.316(b)(1)** |
| Time Limit | **164.316(b)(2)(i)** |
| Availability | **164.316(b)(2)(ii)** |
| Updates | **164.316(b)(2)(iii)** |

PYLON TECHNOLOGY

Your Technology Advisor