ARRAKIS

HIPAA Case Studies: ISO 27001 Overlap and Negligence Considerations Governance

Arrakis Consulting







Purpose

This document presents three practical HIPAA case studies showing how an ISO/IEC 27001 information security management system (ISMS) can reinforce protection of electronic protected health information (ePHI). It also explains how the U.S. Department of Justice (DOJ) Federal Sentencing Guidelines make documented compliance programs, risk management, training, reporting, and corrective action relevant when negligence or organizational misconduct is evaluated.

HIPAA is a legal and regulatory requirement for covered entities and business associates. ISO/IEC 27001 is a voluntary management-system standard. ISO 27001 certification does not establish HIPAA compliance, but its risk-based governance, control structure, and audit evidence can substantially support a HIPAA program.

Case Study 1: Multi-Clinic Network Addresses Weak Access Controls

Situation

A regional clinic network discovered that former employees retained access to electronic health record systems and shared administrative accounts were used by support staff. An internal review found incomplete access reviews, inconsistent termination procedures, and limited evidence of workforce training.

Actions Taken

- Completed a HIPAA Security Rule risk analysis focused on ePHI systems, users, threats, vulnerabilities, and likely impact.
- Eliminated shared accounts and enforced unique user IDs, multi-factor authentication, role-based access, and rapid termination procedures.
- Implemented quarterly access reviews and retained evidence of approvals, removals, and exceptions.
- Updated workforce security and HIPAA training, including sanctions for policy violations.
- Tested incident reporting and breach-escalation procedures.

Results

The clinic network improved visibility into access to ePHI, reduced orphaned accounts, and created a repeatable control-evidence process for leadership, auditors, and business partners.

Cross-References

- **HIPAA:** Security Rule administrative safeguards for risk analysis, workforce security, information access management, security awareness and training, and evaluation; technical safeguards for access control, audit controls, authentication, and transmission security.

- **ISO/IEC 27001:** ISMS scope, risk assessment and treatment, access control, identity management, logging and monitoring, human-resource security, incident management, and internal audit.
- **Overlap:** Both approaches require management accountability, risk-based control selection, documented procedures, access governance, review cycles, and evidence that controls operate as designed.
- **DOJ negligence considerations:** A known access-control weakness that remains unaddressed can support an argument that the organization failed to exercise reasonable care. Documented risk acceptance, remediation ownership, deadlines, leadership oversight, and verification provide stronger evidence of a good-faith compliance effort.

Case Study 2: Hospital Strengthens Business Associate and Ransomware Readiness

Situation

A hospital relied on multiple vendors for billing, cloud hosting, transcription, and managed IT. A ransomware event at a vendor interrupted a service containing ePHI. The hospital had agreements in place, but vendor-risk records were incomplete and incident-notification expectations were not consistently tested.

Actions Taken

- Created an inventory of business associates, data flows, system dependencies, and ePHI access paths.
- Standardized business associate agreements with security requirements, permitted-use limits, breach-reporting timelines, subcontractor obligations, and cooperation requirements.
- Established supplier due diligence, annual reassessments, risk ratings, and corrective-action tracking.
- Updated the incident response plan to include ransomware containment, evidence preservation, communications, recovery, and HIPAA breach-assessment steps.
- Conducted a tabletop exercise with executive leaders, IT, privacy, legal, communications, and the affected vendor.

Results

The hospital gained clearer accountability across its vendor ecosystem, improved recovery coordination, and generated evidence of preparedness before a live incident.

Cross-References

- **HIPAA:** Privacy Rule limits on uses and disclosures; Security Rule risk management, contingency planning, security incident procedures, and business associate safeguards; Breach Notification Rule assessment and notification obligations.

- **ISO/IEC 27001:** Supplier relationship security, cloud-service governance, threat and vulnerability management, incident planning and response, information backup, business continuity, and continual improvement.
- **Overlap:** HIPAA business associate management and ISO 27001 supplier security both require organizations to define security expectations, assess third parties, monitor performance, and retain supporting records.
- **DOJ negligence considerations:** The Federal Sentencing Guidelines emphasize effective compliance and ethics programs, including oversight, training, reporting mechanisms, monitoring, enforcement, and timely corrective action. Failure to investigate, preserve evidence, or remediate known vendor risks may increase organizational exposure when misconduct or negligence is assessed.

Case Study 3: Telehealth Provider Improves Governance After Inappropriate Disclosure

Situation

A telehealth provider used collaboration tools and cloud storage to coordinate patient services. A staff member inadvertently shared a file containing patient information with an unauthorized recipient. Investigation showed inconsistent data-classification practices, no documented secure-sharing standard, and limited monitoring of external file-sharing activity.

Actions Taken

- Conducted an incident investigation, documented the facts, and completed a HIPAA breach risk assessment.
- Implemented data classification and handling rules for ePHI, including approved collaboration and file-transfer tools.
- Enforced encryption, external-sharing restrictions, data-loss prevention settings, and audit logging.
- Delivered role-based training for clinical, administrative, and technical teams.
- Established corrective-action plans, effectiveness reviews, and executive reporting for recurring privacy and security risks.

Results

The provider improved control over ePHI sharing, strengthened employee accountability, and built an auditable process for identifying, investigating, correcting, and learning from privacy events.

Cross-References

- **HIPAA:** Privacy Rule minimum-necessary standard; Security Rule policies and procedures, security awareness training, audit controls, integrity, transmission security, and evaluation; Breach Notification Rule risk assessment where an impermissible use or disclosure occurs.

- **ISO/IEC 27001:** Information classification, acceptable use, data leakage prevention, cryptography, logging, awareness and training, incident management, nonconformity, corrective action, and management review.
- **Overlap:** Both HIPAA and ISO 27001 expect organizations to move beyond policy statements by training personnel, monitoring controls, investigating failures, documenting corrective actions, and checking whether remediation works.
- **DOJ negligence considerations:** An isolated human error is evaluated differently from a pattern of ignored warnings, inadequate training, absent reporting channels, or failure to correct recurring issues. Evidence of prompt investigation, proportionate discipline, remediation, and oversight helps demonstrate that the organization took compliance obligations seriously.

DOJ Federal Sentencing Guidelines: Practical Relevance

The DOJ Federal Sentencing Guidelines for organizations are not a HIPAA control catalog. However, they provide a useful framework for evaluating whether an organization maintained an effective compliance and ethics program. In negligence-related situations, the strength of the organization's governance and response can be highly relevant.

Key program elements include:

- Board or senior-leadership oversight of compliance and risk.
- Clear standards, policies, procedures, and delegated responsibility.
- Reasonable screening and role assignment practices.
- Practical, recurring training and effective communication.
- Confidential reporting channels and non-retaliation expectations.
- Monitoring, auditing, risk assessment, and periodic program evaluation.
- Consistent enforcement, including appropriate disciplinary measures.
- Prompt investigation, remediation, and program improvement after identified issues.

Implementation Takeaways

- Treat HIPAA risk analysis as an ongoing management activity, not a one-time assessment.
- Use ISO/IEC 27001 to organize governance, risk treatment, control ownership, internal audit, and continual improvement.
- Maintain evidence: risk registers, policies, training records, access reviews, vendor reviews, incident reports, tabletop results, corrective-action plans, and management-review decisions.
- Escalate material risks to leadership, assign owners and due dates, and document risk acceptance when remediation cannot be immediate.
- Test incident response and business continuity procedures before an actual breach or outage.

Conclusion

HIPAA establishes specific protections for PHI and ePHI, while ISO/IEC 27001 offers a disciplined, risk-based system for managing information security across people, processes, technology, and suppliers. Together, they help organizations reduce exposure, improve audit readiness, and demonstrate diligence. A documented and actively managed compliance program—supported by leadership oversight, training, monitoring, reporting, enforcement, and corrective action—also provides important evidence that the organization worked to prevent negligent conduct rather than merely reacting after harm occurred.

This material is educational and should be tailored with qualified legal and compliance counsel to an organization's facts, jurisdiction, contracts, and regulatory obligations.

Arrakis Consulting, LLC

.

Ready to get started?

Reach out to use at your earliest convenience to get your company closer to compliance, pass a certifying audit, reduce risk, or increase the skillsets of your personnel.

sales@arrakisconsulting.com

www.arrakisconsulting.com