DAShealth™

www.DAShealth.com

How to Navigate the HIPAA Security Rule Changes

Introduction

STAYING COMPLIANT WITH HEALTHCARE DATA REGULATIONS

Healthcare organizations must continuously protect patient information and meet regulatory requirements. Recent updates to federal and state laws, including changes to the HIPAA Security and Privacy Rules, alignment with 42 CFR Part 2, and new safeguards for reproductive health information, emphasize the need for strong data privacy and cybersecurity practices.

This guide outlines key regulatory changes and provides actionable steps to help healthcare organizations meet compliance requirements. From enhancing cybersecurity measures to adapting to state-specific health data laws, each section offers practical insights for protecting sensitive patient information.

Stay informed, protect patient data, and ensure compliance—today and in the future.

Strengthening Cybersecurity Measures

SUMMARY

The Department of Health and Human Services (HHS) has proposed modifications to the HIPAA Security Rule to enhance cybersecurity protections. These changes aim to address the increasing threats to ePHI and include:

- Mandatory Encryption: All ePHI must be encrypted to protect data confidentiality and integrity.
- Multi-Factor Authentication (MFA): Implementing MFA is required to ensure that only authorized personnel can access ePHI.
- Regular Security Audits: Organizations must conduct periodic security assessments to identify and address vulnerabilities.

RECOMMENDED ACTIONS ↘

RECOMMENDED ACTIONS

- **Assess Current Security Measures**: Evaluate existing encryption protocols and authentication processes to ensure they meet the new standards.

- **Implement MFA:** Adopt MFA solutions for systems accessing ePHI to add an extra layer of security.

- **Implement Strict Role-Based Access Controls (RBAC):** Document your roles and implement role-based access in your systems based on roles and least privilege access.

- **Implement Automatic Access Revocation:** Evaluate and implement methods to automate access revocation when staff leaves the organization.

- **Conduct Regular Vulnerability Scanning** (at least every six months): Conduct automated vulnerability scans to identify technical vulnerabilities in the covered entity's or business associate's relevant electronic information systems.

- **Conduct Annual Penetration Testing**: Penetration testing must be performed at least once every 12 months.

- **Have an Incident Response and Recovery Plan in Place:**
  - Develop a business continuity and disaster recovery plan
  - Develop an incident response plan
  - Test the plans regularly

- **Evaluate Your Business Associates:** Conduct annual evaluations of your Business Associates ensuring they are compliant with HIPAA Security and Privacy rules.

- **Schedule Regular Audits:** Establish a routine schedule for comprehensive security audits and promptly address any identified issues.

Updates to HIPAA Privacy Rule

SUMMARY

Proposed changes to the HIPAA Privacy Rule aim to improve patient access to their health information and facilitate coordinated care. Key updates include:

- Shortened Response Time: The timeframe for healthcare providers to respond to patient requests for access to their health records has been reduced.
- Fee Limitations: There are now caps on the fees that can be charged to patients for accessing their health information.

RECOMMENDED ACTIONS

- **Review and Update Policies:** Ensure that internal policies align with the new response times and fee structures.
- **Staff Training:** Educate staff on the updated procedures to ensure timely and compliant responses to patient requests.

DAShealth™

Alignment with 42 CFR Part 2

SUMMARY

The Confidentiality of Substance Use Disorder Patient Records regulations (42 CFR Part 2) have been updated to align more closely with HIPAA. This change simplifies the sharing of substance use disorder treatment records among healthcare providers while maintaining patient privacy protections.

RECOMMENDED ACTIONS

- **Update Consent Forms:** Revise consent forms to reflect the changes and ensure they are compliant with both HIPAA and 42 CFR Part 2.

- **Educate Staff:** Provide training on the new guidelines to ensure proper handling and sharing of substance use disorder treatment records.

Protection of Reproductive Health Information

SUMMARY

New regulations have been introduced to safeguard reproductive health information, particularly in response to evolving state laws and technological tracking methods like geofencing.

RECOMMENDED ACTIONS

- **Review Data Collection Practices:** Ensure that data related to reproductive health is collected, stored, and shared in compliance with the new regulations.

- **Implement Geofencing Restrictions:** Avoid using geofencing technologies around sensitive areas to prevent unauthorized data collection.

Compliance with State-Specific Health Data Laws

SUMMARY

Several states have enacted laws regulating the collection of health and fitness data, extending beyond federal HIPAA requirements.

RECOMMENDED ACTIONS

- **Stay Informed:** Keep abreast of state-specific regulations that may affect your organization's data collection and sharing practices.

- **Adjust Policies Accordingly:** Modify data handling procedures to comply with both federal and state laws.

Have You Completed the Recommended Actions for Each Category?

□ Strengthening Cybersecurity Measures

□ Updates to HIPAA Privacy Rule

□ Alignment with 42 CFR Part 2

□ Protection of Reproductive Health Information

□ Compliance with State-Specific Health Data Laws

DAShealth™

Connect with Healthcare Cybersecurity Experts

Website

www.DAShealth.com

Phone Number

813-774-9800 x2

Email

Info@DAShealth.com

A-LIGN SOC 2

2025 WINNER CYBER SECURITY EXCELLENCE AWARDS