DIS Direct HIPAA Security and Breach Notification Rule Assessment

2024 Assessment of HIPAA Compliance

Report As-of Date: 10-2-2024

Table of Contents

Introduction

Objectives

DIS Direct performed an assessment of the controls in place to satisfy the requirements of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, as well as the requirements of the Breach Notification Rule as formalized by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 and the Omnibus Rule of 2013. The specific objective of the assessment included the evaluation of the controls in place for protecting the confidentiality, integrity, and availability of protected health information (PHI) to satisfy the requirements of the HIPAA Security Rule and the HIPAA Breach Notification Rule.

HIPAA Security and Breach Notification Rules

The HIPAA Security Rule specifically focuses on the safeguarding of PHI through the implementation of administrative, physical, and technical safeguards. Compliance is mandated to all organizations defined by HIPAA as a covered entity and a business associate. These organizations are required to:

- Ensure the confidentiality, integrity, and availability of all PHI that it creates, receives, maintains, or transmits.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
- Protect against reasonably anticipated unauthorized uses or disclosures of protected health information (PHI).
- Ensure compliance by its workforce.

The requirements of the HIPAA Security Rule are organized according to safeguards, standards, and implementation specifications. The major sections include:

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Organizational Requirements
- Policies and Procedures and Documentation Requirements

The HIPAA Breach Notification Rule, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured PHI. The major sections of the rule include:

- Notification in the Case of Breach
- Notification to the Media
- Notification to the Secretary
- Notification by a Business Associate
- Law Enforcement Delay

Assessment Scope and Methodology

Assessment Approach

The assessment conducted by DIS Direct incorporated the review of artifacts including policies and procedures, system configurations, and sample evidence. Through this review, DIS Direct determined whether the design and implementation of the controls were reasonable and appropriate to meet the requirements associated with the HIPAA Security and Breach Notification Rule.

Assessment Limitations

Although it is impossible for any assessment of controls or security to guarantee complete assurance or 100 percent protection against control failures or security breaches, it is essential to understand that conclusions on specific controls and security measures have inherent limitations. As a result, errors or fraud may occur and go unnoticed. Additionally, it is essential to recognize that information networks, applications, and control environments are always evolving, and DIS Direct's examination of DIS Direct control and security methods and procedures is limited to a specific point in time. Thus, any conclusions based on DIS Direct assessment are subject to risks that include changes to the systems or controls, modifications in processing requirements, the passage of time, or the discovery of new security exploits that may alter the validity of DIS Direct conclusions.

DIS Direct Overview

DIS Direct is a DIS Direct is a leader in personalized and customized direct mail campaigns, delivering high-volume postcards and self-mailers via the US Postal Service. They offer personalized messaging through a blend of traditional print and digital technologies. This report

exclusively covers the services provided by DIS Direct, which is acting as a Business Associate (BA) under HIPAA.

Scope of the Assessment

This assessment considered three (3) fundamental security parameters: confidentiality, integrity, and availability. This assessment reviewed the use, disclosure, and accessibility of protected health information (PHI) and PHI available to authorized individuals. This assessment reviewed the standards and implementation specifications of the HIPAA Security Rule and Breach Notification Rule.

The scope of this review included:

1. DIS Direct policies and procedures related to HIPAA Compliance.
2. DIS Direct information system(s) and platform(s) maintaining PHI.

Executive Summary

Conclusion

DIS Direct's compliance intentions are established through the design and implementation of administrative, technical, and physical controls throughout the infrastructure and supporting processes.

Based on documentation inspection, inquiry, and observation of control effectiveness, DIS Direct noted the result of the assessment was: **Satisfactory**

Result	Definition
Satisfactory	DIS Direct has completed the assessment without significant findings and concluded that the organization has implemented safeguards to satisfy the requirements set forth by the regulation.

Summary Results

The table below provides a high-level overview of compliance for the environment. Each of the compliance requirements was determined to be met with a satisfactory rating. In the event a compliance requirement was not deemed satisfactory, it was determined to not apply to DIS Direct given the nature and operation of the business. As noted within the “Conclusion” section above, the overall rating of the assessment was: **Satisfactory**.

Administrative Safeguards		
Standard	**Regulation**	**Title**
Security Management Process	164.308(a)	Security management process
	164.308(a)(1)(ii)(A)	Risk analysis
	164.308(a)(1)(ii)(B)	Risk management
	164.308(a)(1)(ii)(C)	Sanction policy
	164.308(a)(1)(ii)(D)	Information system activity review
Assigned Security Responsibility	164.308(a)(2)	Assigned security responsibility
Workforce Security	164.308(a)(3)(i)	Workforce security
	164.308(a)(3)(ii)(A)	Authorization and/or supervision
	164.308(a)(3)(ii)(B)	Workforce clearance procedure
	164.308(a)(3)(ii)(C)	Termination procedures
Information Access Management	164.308(a)(4)(i)	Information access management
	164.608(a)(4)(ii)(A)	Isolating healthcare clearinghouse functions
	164.308(a)(4)(ii)(B)	Access authorization
	164.308(a)(4)(ii)(C)	Access establishment and modification
Security Awareness and Training	164.308(a)(5)(i)	Security awareness and training
	164.308(a)(5)(ii)(A)	Security reminders
	164.308(a)(5)(ii)(B)	Protection from malicious software
	164.308(a)(5)(ii)(C)	Log-in monitoring
	164.308(a)(5)(ii)(D)	Password management

Security Incident Procedures	164.308(a)(6)(i)	Security incident procedures
	164.308(a)(6)(ii)	Response and reporting
Contingency Plan	164.308(a)(7)(i)	Contingency plan
	164.308(a)(7)(ii)(A)	Data backup plan
	164.308(a)(7)(ii)(B)	Disaster recovery plan
	164.308(a)(7)(ii)(C)	Emergency mode operation plan
	164.308(a)(7)(ii)(D)	Testing and revision procedures
	164.308(a)(7)(ii)(E)	Applications and data criticality analysis
Evaluation	164.308(a)(8)	Evaluation
Business Associate Contracts and Other Arrangements	164.308(b)(2)	Business associate contracts and other arrangements
	164.308(b)(3)	Written contract or other arrangement
Physical Safeguards		
Facility Access Controls	164.310(a)(1)	Facility access controls
	164.310(a)(2)(i)	Contingency operations
	164.310(a)(2)(ii)	Facility security plan
	164.310(a)(2)(iii)	Access control and validation procedures
	164.310(a)(2)(iv)	Maintenance records
Workstation Use	164.310(b)	Workstation use
Workstation Security	164.310(c)	Workstation security
Device and Media Controls	164.310(d)(1)	Device and media controls
	164.310(d)(2)(i)	Disposal
	164.310(d)(2)(ii)	Media re-use
	164.310(d)(2)(iii)	Accountability
	164.310(d)(2)(iv)	Data backup and storage
Technical Safeguards		
Access Control	164.312(a)(1)	Access control
	164.312(a)(2)(i)	Unique user identification
	164.312(a)(2)(ii)	Emergency access procedure
	164.312(a)(2)(iii)	Automatic logoff
	164.312(a)(2)(iv)	Encryption and decryption
Audit Controls	164.312(b)	Audit controls
Integrity	164.312(c)(1)	Integrity

	164.312(c)(2)	Mechanism to authenticate protected health information
Person or Entity Authentication	164.312(d)	Person or entity authentication
Transmission Security	164.312(e)(1)	Transmission security
	164.312(e)(2)(i)	Integrity controls
	164.312(e)(2)(ii)	Encryption
Organizational Safeguards		
Business Associate Contracts or Other Arrangements	164.314(a)	Business associate contracts or other arrangements
Requirements for Group Health Plans	164.314(b)(1)	Requirements for group health plans
Policies and Procedures Documentation Requirements		
Policies and Procedures	164.316(a)	Policies and procedures
Documentation	164.316(b)(1)	Documentation
	164.316(b)(2)(i)	Time limit
	164.316(b)(2)(ii)	Availability
	164.316(b)(2)(iii)	Updates
Breach Notification Rule		
Breach Notification	164.404(a)	Individual notification
	164.404(b)	Timeliness of notification
	164.404(c)	Content of notification
	164.404(d)	Written or electronic notification
	164.406	Media notification
	164.408	Secretary notification
	164.410	Business associate notification
	164.412	Notification delay request of law enforcement
	164.414	Burden of proof