PHI Data breach Notification Procedure

Version 1 - Approved by Youssef Ouyhya

Contents

1. Objective

The PHI Data Breach Notification Procedure outlines the steps to be followed in the event of a breach of Protected Health Information (PHI) as required by HIPAA regulations. The procedure aims to ensure timely and appropriate notification to affected individuals, regulatory authorities, and other relevant parties to minimize harm and uphold the privacy and security of PHI.

2. Scope

This procedure applies to all employees, contractors, and business associates of CNTXT who handle or have access to PHI. It covers all breaches involving the unauthorized access, acquisition, use, disclosure, or destruction of PHI in any form or medium.

3. PHI Data Breach Notification Procedure

3.1 Definitions

- Protected Health Information (PHI): PHI refers to individually identifiable health information transmitted or maintained in any form or medium, including electronic, oral, or written records, that is created or received by a covered entity or business associate and relates to the past, present, or future physical or mental health condition of an individual, provision of healthcare, or payment for healthcare.
- Breach: A breach is defined as the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule, which compromises the security or privacy of the information.

3.2 Reporting a Potential Breach

- Any employee, contractor, or business associate at CNTXT who becomes aware of a potential breach of PHI must immediately report it to the designated Privacy Officer or the Information Security Officer.
- The report should include details such as the date, time, and description of the incident, the type of PHI involved, and any known or suspected causes.

3.3 Assessment and Investigation

- The Privacy Officer or the Information Security Officer will promptly initiate an assessment and investigation upon receiving a potential breach report.
- The investigation will determine if a breach has occurred, evaluate the extent of the breach, identify affected individuals, assess potential risks and harms, and establish the cause and source of the breach.

3.4 Breach Determination

Based on the findings of the investigation, the Privacy Officer or the Information Security Officer will determine whether a breach has occurred, considering the four factors specified by HIPAA: (1) the nature and extent of the PHI involved, (2) the unauthorized person who used the PHI or to whom the disclosure was made, (3) whether the PHI was actually acquired or viewed, and (4) the extent to which the risk to the PHI has been mitigated.

If it is determined that a breach has occurred, the notification process will be initiated.

3.5 Notification Process

Notification to Affected Individuals:

- Upon confirming a breach of PHI and identifying affected individuals, CNTXT will provide written notification to each affected individual without unreasonable delay, but no later than 60 days after discovering the breach, unless a law enforcement delay is requested.
- The notification will include a description of the breach, the type of PHI involved, steps individuals should take to protect themselves, a description of actions taken by the organization to investigate and mitigate the breach, and contact information for further inquiries.

3.6 Notification to Regulatory Authorities

- CNTXT will comply with all applicable legal requirements for reporting breaches to the relevant regulatory authorities.
- The Privacy Officer or the designated representative will be responsible for submitting the required notifications within the specified timeframes.
- Media and Public Communication: CNTXT will establish a communication plan to address media inquiries, public statements, or press releases

4. Document Security Classification

Company Internal (please refer to the Data Classification policy for details).

5. Non-Compliance

Compliance with this policy shall be verified through various methods, including but not limited to automated reporting, audits, and feedback to the policy owner. Any staff member found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment or contractual agreement. The disciplinary action shall depend on the extent, intent, and repercussions of the specific violation.

6. Responsibilities

The Information Security Officer is responsible for approving and reviewing policy and related procedures. Supporting functions, departments, and staff members shall be responsible for implementing the relevant sections of the policy in their area of operation.

7. Schedule

This document shall be reviewed annually and whenever significant changes occur in the organization.

End of PHI Data Breach Notification Procedure. For version history, please see the next page.

Version history

Version	Log	Date
1 Current	Policy version approved by Youssef Ouyhya	26 Oct, 2024
1	New Policy version Created	26 Oct, 2024