## **Data Security Breach Reporting and Response Policy**

## **1. Purpose**

The purpose of this policy is to establish a comprehensive framework for reporting and responding to data security breaches involving Protected Health Information (PHI) and other sensitive data. This policy aims to protect the confidentiality, integrity, and availability of data, ensure compliance with applicable laws and regulations, and minimize the impact of breaches on affected individuals and the organization.

## **2. Scope**

This policy applies to all employees, contractors, and agents of **[Organization Name]** who have access to PHI and other sensitive data. It covers all types of data breaches, including electronic, paper, and verbal breaches.

## **3. Definitions**

* **Data Security Breach:** Any unauthorized access, acquisition, use, or disclosure of PHI or other sensitive data that compromises the privacy or security of the data.
* **Protected Health Information (PHI):** Any individually identifiable health information that is transmitted or maintained in any form or medium, including oral, written, or electronic.
* **Incident Response Team (IRT):** A designated group of individuals responsible for managing and responding to data security breaches and incidents.

## **4. Policy Statement**

**[Organization Name]** is committed to maintaining the security and privacy of PHI and sensitive data. In the event of a data security breach, all employees must adhere to the procedures outlined in this policy to ensure timely and effective reporting and response.

## **5. Roles and Responsibilities**

### **5.1 Employees**

* All employees must be aware of their responsibility to report any suspected or confirmed data security breaches immediately.
* Employees should be trained to recognize potential security breaches and understand the reporting process.

### **5.2 Data Security Officer (DSO)**

* The DSO is responsible for overseeing the implementation of this policy, ensuring compliance with applicable laws and regulations, and serving as the primary contact for breach-related issues.
* The DSO will coordinate the investigation and response to reported breaches.

### **5.3 Incident Response Team (IRT)**

* The IRT will consist of representatives from various departments, including IT, legal, compliance, and communications.
* The IRT will be responsible for assessing the breach, determining the appropriate response, and managing communication with affected individuals and regulatory bodies.

## **6. Breach Identification and Reporting**

### **6.1 Identification of a Breach**

Employees must report any suspected or confirmed data security breaches, including but not limited to:

* Unauthorized access to PHI or sensitive data
* Loss or theft of devices containing PHI (e.g., laptops, mobile devices, paper records)
* Inadvertent disclosure of PHI to unauthorized individuals or entities
* Malware attacks, phishing attempts, or other cyber threats

### **6.2 Reporting Process**

* **Immediate Reporting:** Employees must report any suspected or confirmed breaches to the Data Security Officer (DSO) within **[insert time frame, e.g., 24 hours]** of discovery.
* **Reporting Method:** Reports can be made verbally or in writing, using the designated reporting form available on the organization’s intranet or by contacting the DSO directly.
* **Information to Include:** Reports should include the following information, if known:

o Date and time of the breach

o Description of the breach (e.g., nature of the unauthorized access or disclosure)

o Types of data involved (e.g., patient names, Social Security numbers)

o Individuals or entities affected by the breach

o Any immediate actions taken to mitigate the breach

## **7. Breach Investigation and Assessment**

### **7.1 Investigation**

* Upon receiving a breach report, the DSO will initiate an investigation to assess the nature and extent of the breach.
* The investigation will include gathering evidence, interviewing relevant personnel, and determining whether the breach involves PHI or other sensitive data.

### **7.2 Risk Assessment**

* The IRT will conduct a risk assessment to evaluate the potential harm to affected individuals and the organization.
* Factors to consider in the risk assessment may include:

o The nature and scope of the data involved

o The likelihood of re-identification of de-identified data

o The context of the breach (e.g., unauthorized access, inadvertent disclosure)

o Any security measures in place to protect the data

* Based on the risk assessment, the IRT will determine whether the breach constitutes a reportable incident under HIPAA or applicable state laws.

## **8. Notification Requirements**

### **8.1 Individual Notification**

* If the breach involves PHI and poses a significant risk of harm, **[Organization Name]** will notify affected individuals without unreasonable delay and no later than **[insert time frame, e.g., 60 days]** after the breach is discovered.
* Notification will be provided in writing and may include:

o A description of the breach and the types of PHI involved

o Steps individuals can take to protect themselves from potential harm

o Contact information for questions or concerns

### **8.2 Regulatory Notification**

* If required by HIPAA or state laws, the DSO will notify the U.S. Department of Health and Human Services (HHS) and relevant state agencies within the required time frames.
* Notification to HHS will be made through the HIPAA Breach Reporting Tool.

### **8.3 Media Notification**

If the breach affects a large number of individuals (typically 500 or more), the organization will notify prominent media outlets in accordance with regulatory requirements.

## **9. Remedial Actions**

### **9.1 Corrective Actions**

The IRT will recommend and implement corrective actions to prevent future breaches, which may include:

* Enhancing security measures
* Conducting employee training and awareness programs
* Revising policies and procedures

### **9.2 Documentation**

All breaches and responses will be documented, including:

* Details of the breach
* The investigation process
* Risk assessment results
* Notifications made to individuals and regulatory bodies
* Corrective actions taken

Documentation will be retained for a minimum of **[insert time frame, e.g., six years]** or as required by applicable laws.

## **10. Training and Awareness**

### **10.1 Employee Training**

All employees will receive training on this policy and data security breach reporting procedures upon hire and annually thereafter.

Training will include:

* Recognizing potential data security breaches
* Understanding reporting obligations
* Knowing the importance of data protection

### **10.2 Policy Review**

This policy will be reviewed annually or as needed to ensure compliance with changes in HIPAA regulations and organizational practices.

## **11. Enforcement**

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment. Legal action may also be pursued if violations result in harm to individuals or the organization.