

<b>Title:</b>	<b>ISF 6.0 – Incident Management Policy</b>	<b>Effective Date:</b>	<b>12/28/2020</b>
<b>Author:</b>	<b>Haroon Ahmad</b>	<b>Last Review Date:</b>	<b>12/22/2021</b>
<b>Location:</b>	<b>All Locations</b>	<b>Last Revision Date:</b>	<b>12/22/2021</b>
<b>Functional Area:</b>	<b>All Locations</b>		

## CONTENTS

<b>6.0</b>	<b>Incident Management Policy</b>	<b>1</b>
6.1	<i>Purpose</i>	1
6.2	<i>Scope</i>	1
6.3	<i>Policy</i>	1
6.3.1	Incident Definition	1
6.3.2	Incident Identification	1
6.3.3	Incident Response Steps	2
6.3.4	Incident Documentation & Tracking	3

## **6.0** INCIDENT MANAGEMENT POLICY

### **6.1** **PURPOSE**

This policy defines the processes in place at Liberty Healthcare Corporation and its affiliates (Liberty) to properly ensure that all incidents involving Liberty data and information assets, technologies, services, applications are properly investigated and appropriately tracked to detect and limit the impact to any data confidentiality, integrity, or availability.

Proper tracking, response, and investigation of a potential or verified incident will help prevent the propagation of an incident, as well as provide sufficient information to prevent an incident from reoccurring.

### **6.2** **SCOPE**

This policy applies to all applications owned, managed, used and/or developed by Liberty including any Liberty owned or managed data in any format.

### **6.3** **POLICY**

#### **6.3.1** **INCIDENT DEFINITION**

An incident is defined as any adverse event that compromises an aspect of Liberty Healthcare’s network, data, controls, functionality, or business operations. An incident may originate from either an external or internal source and may also be as a result of inadvertent act or an intentional attack.

#### **6.3.2** **INCIDENT IDENTIFICATION**

All Liberty employees should be aware of the potential symptoms of a possible incident. An intrusion incident could result in symptoms if a system is compromised by an external attack (i.e. virus, malware, worm, etc.). These symptoms include excessive pop-up messages, reduced system performance, unknown files or directories, modified websites, full disk drives, etc. These incidents

may also be uncovered through manual reviews or automated means such as protection software, audit logs, vulnerability reports, third party assessments, and more.

Additional incidents are defined as any unauthorized disclosure of any company data. This can result from an external attack as well as an internal misuse - such as unauthorized data access through accidental sharing, data stored in an incorrect directory, or purposeful unapproved data access. Similarly, HIPAA incidents can be defined as any incident where PHI information is exposed in an unauthorized manner for any data type - digital or physical. The Liberty Privacy Officer must be notified for HIPAA related incidents.

#### 6.3.2.1 INCIDENT CLASSIFICATION

All incidents should be classified based on their severity. The incident severity may change as the incident response process is advanced.

The severity levels are:

**Low** – Limited effect to confidentiality or availability of data, services, or operations.

**High** – A possible substantial effect to the confidentiality or availability of data, services, or operations.

**PHI/PII** – This additional designation is for an incident that may include the unauthorized access of PHI information. A PHI/PII incident may also be designated as either Low or High (as described above) to address specific regulatory or contractual data count exposure limits.

### 6.3.3 INCIDENT RESPONSE STEPS

#### 6.3.3.1 REPORTING A POSSIBLE INCIDENT

All Liberty employees and staff are expected to report any suspected or confirmed incident. **Any incident (confirmed or suspected) that risks exposure of Liberty proprietary or confidential information, including any exposure risk of PHI, should be considered urgent and must be reported immediately in order to remediate and minimize an exposure.** Examples would include a compromised email account or password, a suspect phishing attempt, or the suspicion someone has gained unauthorized access to any Liberty information technology asset or proprietary information. Reporting can be affected by sending an email to [security@libertyhealth.com](mailto:security@libertyhealth.com), submitting a Zendesk ticket, or phoning any member of the Technology Solutions team, up to and including the ISO or CIO.

All Incidents (urgent or not) should be reported to Liberty's Information Security Officer (ISO) and Corporate Compliance Officer at the earliest convenience. Any pertinent information regarding the incident should be emailed to [security@libertyhealth.com](mailto:security@libertyhealth.com).

#### 6.3.3.2 INFORMATION GATHERING

The Liberty Technology Solutions in conjunction with the Information Security Officer will gather as much information as possible through interviews and system reviews to evaluate the potential scope of the incident. Interviews will be conducted to understand the incident's origination, the effect on business operations or services, as well as any other critical details such as individuals involved, affected users or systems, possible damage, potential illegal activity, forgery, fraud, misrepresentation, or any other critical details that may be deemed applicable.

#### 6.3.3.3 LIMIT INCIDENT EXPOSURE

Liberty Technology Solutions in conjunction with the Information Security Officer and Compliance Officer, will first work to limit the expansion of the incident. This can be achieved by a variety of methods such as temporarily disabling user accounts for any corporate application or service, business services, internet access, mobile devices, phone systems, or any other method deemed necessary.

Notification to third parties may be required to prevent propagation of a potential incident outside of the Liberty networks.

#### **6.3.3.4 INCIDENT IMPACT INVESTIGATION**

Once the incident has been stopped from propagating, Liberty Technology Solutions will begin a review all accounts, services, devices, etc. to determine the potential effect of an incident, to document the details such as the root cause, and to ensure the incident cannot reinitiate. This process includes verification that no accounts have received unauthorized changes, reviewing of log files, verification of system configuration files and software, scanning for possible viruses, malware, worms, or trojans.

#### **6.3.3.5 HIPAA INCIDENT INVESTIGATION**

Liberty Technology Solutions will also investigate any potential data accessed by unauthorized individuals as well as any potential data losses, in coordination with Liberty's compliance Officer. PHI information that may be accessed or affected by the incident will be reported to the Information Security Officer and the Compliance Officer for review to comply with any regulatory or contractual obligations pertaining to PHI data handling requirements as well as any potential notification requirements.

#### **6.3.3.6 INCIDENT MITIGATION AND PREVENTION**

Once the incident investigation is complete, Liberty Technology Solutions and the Information Security Officer will identify methods to mitigate the effect of the current incident as well as to prevent similar incidents from occurring in the future.

### **6.3.4 INCIDENT DOCUMENTATION & TRACKING**

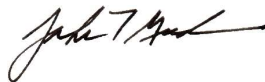
All documentation, analysis, and collected evidence must be retained and tracked appropriately – general information regarding the incident in Liberty's incident tracking system, and more detailed or technical information in the incident reporting system. Maintaining incident information allows for additional metrics and reference capability to provide better awareness in the event of a repetitive or similar incident.

The Information Security Officer must review the final report for completion of information as well as ensure all appropriate aspects of the incident have been reviewed and investigated to completion. The report should also document corrective actions that have been implemented as a result of the incident. The Compliance Officer must review HIPAA related incidents involving PHI data. Once the reports are reviewed and deemed satisfactory, the incident can be marked as closed.

### **APPROVALS**



Haroon Ahmad – Information Security Officer



John T. Guda – CIO / CTO

### **REVISION HISTORY**

Version	Date	Author	Summary of Changes
1.0	12/28/2020	Haroon Ahmad	Initial ISF release – refactor and update of previous security policies into distinct documents
2.0	12/22/2021	Haroon Ahmad	Annual Review. Updates made to incident reporting