Liberty Healthcare Corporation and Affiliates (Liberty) Standard Operating Policies

Title:	**ISF 5.0 – Risk Management Policy**	**Effective Date:**	**12/28/2020**
Author:	**Haroon Ahmad**	**Last Review Date:**	**12/22/2021**
Location:	**All Locations**	**Last Revision Date:**	**12/22/2021**
Functional Area:	**All Areas**		

CONTENTS

5.0 RISK MANAGEMENT POLICY

5.1 PURPOSE

This policy defines the requirements pertaining to risk management for Liberty Healthcare Corporation and its affiliates (Liberty), including the process guidelines for performing an appropriate risk assessment review on all of the company's information system assets. The purpose of the risk assessment process is to determine and assess potential risks to the company, and ensure appropriate controls are in place to ensure the confidentiality, integrity, and availability of all Liberty data as required by applicable laws, regulations, frameworks, internal polices, and contractual obligations.

5.2 SCOPE

This policy applies to all computer systems, facilities, third parties, and assets within Liberty with a target audience of executives, program directors, and information technology and security personnel.

5.3 POLICY

5.3.1 RISK ASSESSMENT PROCESS REQUIREMENTS

A risk assessment must be performed for all of Liberty Healthcare's information assets on an annual basis. This includes a review of all of the company's assets, programs, and systems.

Additional risk assessments may be conducted to review changes to any Liberty policies or procedures that are deemed to substantially change a level of risk.

The risk assessment process will be led by the Liberty Information Security Officer (or designee) in conjunction with appropriate parties such as, Liberty Technology Solutions, system owners, data owners, program directors, and executive management.

Results of the risk assessment must be compiled into a report and provided to program directors and executive management to provide an understanding of the potential risks for the company.

Liberty risk assessments must also include the identification of possible fraud, as well as possible risks to the company's compliance with HIPAA (Health Insurance Portability and Accountability Act).

All risks must be tracked through a risk tracker to more easily monitor and view risks for each risk assessment.

The Liberty Health Information Security Officer is responsible for ensuring risk assessments are completed by working with appropriate business managers. The Information Security Officer is also responsible for maintaining any documentation surrounding the risk assessment process.

5.3.2 Risk Assessment Required Steps

5.3.2.1 Asset Identification

A list of all Liberty assets must be compiled. An asset includes any products, systems, services, technologies, applications, data, individuals, as well as any items with an inherited reliance required to perform critical duties.

5.3.2.2 Threat & Vulnerability Identification

A comprehensive list of potential threats to any of the assets defined must be compiled. Threats may range from natural disasters to technology availability, insider threats, fraud, and any other identified vulnerabilities. A threat is determined by the possibility of an unexpected change in the confidentiality, integrity, and/or availability of any system that may negatively affect the company. A threat may be compiled from a variety of sources such as scanning tools, third party assessments, internal evaluations, known system limitations, etc.

5.3.2.3 Controls Analysis

For any identified threats or vulnerabilities, current controls must be in place to limit the potential impact of a successful threat or exploited vulnerability. These controls, should be appropriately reviewed, documented, and considered when determining risk ratings. This analysis will allow for a more accurate view of the associated risk to Liberty Healthcare.

5.3.2.4 Likelihood Analysis

For all the identified threats and vulnerabilities, the likelihood of the threat and/or vulnerability to be realized must also be determined. This likelihood rating should reference the current controls determined in the previous step to ensure a more accurate rating.

This rating should also follow the same qualitative method with Low, Medium, and High likelihood rating levels. The ratings are defined below

High – A threat or vulnerability which is deemed to be highly likely or easily exploited and highly capable of causing material business impact, and current controls in place are not sufficient to limit the threat or vulnerability exploitation from being successful.

Medium – A threat or vulnerability which is deemed to be likely or exploited and capable of causing some business impact, however current controls in place may limit the threat or vulnerability exploitation from being successful.

Low – A threat or vulnerability which is not deemed to be likely or exploited and only capable of causing non-material business impact, and current controls in place are considerably sufficient to limit the threat or vulnerability exploitation from being successful.

5.3.2.5 Impact Analysis

Once assets and relevant threats defined, an analysis must take place to determine the potential impact of a given threat, if successful, to the asset, program, and Liberty as a whole. The impact rating should also include any current controls in place that may limit or mitigate the overall impact of a successful threat to provide a more accurate assessment.

A qualitative analysis score must be given to define the various possible impact rating levels; Low, Medium, High. The ratings are defined below:

High – A successful threat event or exploited vulnerability will lead to the following:

1) Very costly loss of major asset or resource
2) Significant harm, or impediment of the company's mission, reputation, interest, or contractual obligations
3) Result in serious injury or death

Medium – A successful threat event or exploited vulnerability will lead to the following:

1) Costly loss of a major asset or resource
2) Cause harm to or impede the company's mission, reputation, interest, or contractual obligations
3) Result in human injury

Low – A successful threat event or exploited vulnerability will lead to the following:

1) Possible loss of some assets or resources
2) May somewhat affect the company's mission, reputation, interest, contractual obligations

5.3.2.6 Risk Determination

This step is defined to calculate the overall risk rating of a specific threat or vulnerability to an asset of Liberty by referencing the likelihood rating as well as the impact rating determined in the previous steps. An overall risk rating of Low, Medium, or High can be determined by utilizing the matrix figure below.

		Likelihood		
		High	**Medium**	**Low**
Impact	**High**	High	Medium	Low
	Medium	Medium	Medium	Low
	Low	Low	Low	Low

5.3.2.7 Mitigation Control Recommendations

The Information Security Officer (or designee) will work with relevant parties such as Liberty Technology Solutions, business process owners, data owners, system owner, and potentially others to provide executive management with methods of mitigating risks to a lower level as well as potential costs and expected change in rating.

5.3.2.8 Risk Management Options

Once a risk has been appropriately defined and rated, various options are available to manage the risk. The Liberty Information Security Officer, executive management, program directors, and any other relevant parties must be made aware of the determined risk rating prior to selecting a risk option. Options are:

1) Risk Acceptance – The risk and associated risk level are determined to be at an acceptable level.

2) Risk Mitigation – The risk and associated risk level are determined to be too high and must be mitigated to an acceptable level with the implementation of additional controls.
3) Risk Transfer – The risk has been transferred to additional parties to manage the risk.
4) Risk Avoidance – The risk can be redefined with possible changes in rating definitions or change and limit a specific process to avoid the risk entirely.

5.3.3 Risk Remediation

A simple risk report or presentation along with the risk tracker should be provided to appropriate program directors and executive management to provide a clear understanding of the potential risks to Liberty Healthcare.

For any risks where the Risk Mitigation option has been exercised, each mitigation effort and any changes to users, systems, services, business process, internal controls, or others, should be tracked through completion. Meeting minutes and/or Technology Solutions Support tickets should be utilized when appropriate to track changes through completion of change testing and implementation.

Additionally, previous risk assessments should be reviewed and compared to the current risk assessment to ensure that critical risks have not been overlooked.

5.4 Definitions

the following definitions adapted from NIST SP 800-30 shall be used to clarify how risks, vulnerabilities and threats fit together:

Risk – The net mission impact considering (1) the probability that a threat will exercise (accidentally or intentionally exploited) a vulnerability and (2) the resulting impact if this should occur. Risks arise from legal liability or mission loss due to:

- Unauthorized (malicious or accidental) disclosure, modification, or destruction of information
- Unintentional errors or omissions
- IT disruptions due to natural or man-made disasters
- Failure to exercise due care and diligence in the implementation and operation of the IT systems

Vulnerability – A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of Liberty's security SOPs.

Threat – The potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability:

- Natural threats such as floods, earthquakes, tornadoes, and landslides
- Human threats are enabled or caused by humans and may include intentional (e.g. Network and computer-based attacks, malicious software upload, and unauthorized access to e-PHI) or unintentional (e.g. inadvertent data entry or deletion and inaccurate data entry) actions
- Environmental threats such as power failures, pollution, chemicals, and liquid leakage.

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. No major changes