Liberty Healthcare Corporation and Affiliates (Liberty) Standard Operating Policies

Title:	**ISF 3.0 – Acceptable Use 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

3.0 ACCEPTABLE USE POLICY

3.1 PURPOSE

This policy outlines the acceptable use of computer equipment and systems at Liberty Healthcare Corporation and its affiliates (Liberty) for the purpose of protecting the company, its employees, staff, clients, partners, participants, and third parties, from any illegal or damaging actions by any individuals, whether knowingly or inadvertently. By detailing Liberty computer equipment and systems acceptable use requirements and limitations, the risk of breaches, data exposure or loss, compromising of networks, systems and services, along with possible legal exposures and other unforeseen events, can be limited.

3.2 SCOPE

The scope of the Acceptable Use Policy includes, but is not limited to, all Liberty owned and provided devices such as laptop workstations, desktop workstations, smart phones, mobile devices, applications, services including email systems and internet access as well as any other devices, services, and/or applications utilized by any Liberty clients, customers, and/or affiliates.

3.3 POLICY

3.3.1 GENERAL USE AND OWNERSHIP

All data that users create on company systems remains the property of Liberty Healthcare.

Management does not guarantee the confidentiality or privacy of personal information accessed or stored on any device or service administered by Liberty Healthcare. Employees should exercise good judgment regarding the personal use of company assets.

For security and network maintenance purposes, authorized individuals within Liberty may monitor equipment, systems and network traffic at any time. Liberty reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Employees must not engage in any activity that is illegal under local, state, and federal law while utilizing Liberty owned devices or services.

All new employees, subcontractors, and third parties are required to review and acknowledge this policy prior to accessing any of Liberty's information systems.

Employees are required to complete Liberty's security awareness training as soon as possible upon hire. Employees are also required to complete the security awareness training annually.

3.3.2 Security and Proprietary Information

The information contained on Liberty systems should be classified as either Liberty Public or Liberty Confidential, as defined by corporate confidentiality guidelines, details of which can be found in the Data Management policy. Employees should take all necessary steps to prevent unauthorized access to this information. This also includes a requirement that all employees and staff will protect and physically secure any Liberty devices and data.

Keep passwords secure and do not share accounts or security credentials. Authorized users are responsible for the security of their passwords and accounts.

All users are required to lock the screen of their PC, laptop, or workstation when unattended.

Employees should avoid or must use extreme caution when opening e-mail attachments from unknown senders, which may contain viruses, Trojans, or other forms of malware.

Employees must not use or connect removable storage media to any Liberty owned devices. These include but are not limited to, external hard drives, USB drives, zip drives, CDs, DVDs, etc.

Employees must not export any Liberty owned or purchased software, copywrite material, trade secrets, business leads, business processes, business plans, templates, or intellectual property.

Before transmission of Liberty Confidential Information, including but not limited to PHI, employees must verify the identity of the recipient of the information to prevent any unauthorized disclosure of confidential data.

3.3.3 Email Use & FAX

All Liberty Healthcare employees as well as applicable subcontractors and third parties should maintain Liberty Healthcare provided email addresses.

For employees who may not utilize their liberty email address daily in the normal course of their duties, the Liberty email account should be checked at least weekly to ensure important messages are not missed.

All Liberty Healthcare business communications should be conducted using the Liberty healthcare email address, unless an exception has been explicitly approved (for example, use of a customer provided email account for day-to-day communications). However, all communication of Liberty Healthcare confidential information or private employee information must be limited to the Liberty Healthcare email system only.

Liberty employees must exercise extreme caution when sending confidential information through email or FAX services. PHI data may only be sent to non-Liberty recipients when using the secure email service.

a) Employees should use extremely caution in sending any Liberty Confidential information or any PHI or PII information through email. Employees should use any form of encrypted data

transfer for confidential data transmission such as the Secure Email capability.

b) Email use should be limited to business purposes. Personal use should be kept to a minimum. It is the employee's duty to ensure no confidential information is inappropriately included.

c) Employees must not send unsolicited email messages that are not business related, including the sending of "junk mail", chain mail, or other advertising material to individuals who did not specifically request or expect such material (email spam).

d) Employees must not engage in any outside business using Liberty email.

Employees must not engage in any form of harassment via email or telephone whether through language, frequency, or size of messages.

Employees must not engage in unauthorized use, or forging, of email header information.

Many of the company FAX systems rely on and flow through the company's email services. Therefore, employees must adhere to all email security guidelines for FAX as well.

Any outgoing FAX must utilize a cover page with appropriate sender and recipient information. It is the duty of the sender to verify and ensure the recipient of the FAX is authorized receive the information.

3.3.4 Provision or Use of Third-Party Information Services

Employees should not share, post, or send Liberty Confidential information on any websites, forums, social media, or any other unauthorized platforms.

Employees should not use unauthorized or personal internet services such as personal or non-Liberty email, online data storage services, social media, proxy services, etc. when conducting Liberty business.

Provision of information services, systems or technologies, must be arranged by Liberty Technology Solutions and must be approved by the Liberty ISO.

Liberty Healthcare provided credentials (User ID, email address, password, etc) may not be used to establish or managing unapproved information services.

Employees should not use online services that may limit the bandwidth capacity of Liberty networks such as streaming music, streaming video, high-capacity data upload or download, torrents, etc.

Employees must not use Liberty provided internet services to view, access, engage, or take part in any adult themed content, or to participate in any illegal activity as defined by local, state, or federal agencies.

Non-company owned devices, or visiting equipment, must not be connected to any Liberty networks without permission from the Liberty Technology Services and/or the Information Security Officer. Guest wireless networks may be used for non-company owned devices.

Employees using Liberty provided internet services (including office internet connections and mobile hotspots), must not use any streaming audio or video services unrelated to an authorized Liberty business function.

3.3.5 Portable Devices

All Liberty owned portable devices must always be controlled and accounted for. These devices include (but are not limited to) laptop workstations, USB drives, CDs, storage tapes, mobile phones, internet hotspots.

All portable devices shall be encrypted with the company standard encryption protocol whenever applicable.

All portable devices must be secured with individual passwords or passcodes. The passwords and passcodes must not be shared with anyone other than the assigned owner of the device. All passwords and passcodes must adhere to the minimum company standard detailed in the Access Management Policy.

Liberty employees are responsible for the physical security of assigned devices. Devices must be secured when not in use and must not be left unattended where an unauthorized person could access them.

Employees must report any damage or lost/stolen devices immediately to their supervisor, Liberty Technology Solutions, or the Information Security Officer. In addition, a record of any damaged or lost/stolen device must be promptly entered into the Liberty ticketing system.

Sending or receiving Liberty Confidential Information, including but not limited to PHI, through text messaging to any other messaging services is prohibited.

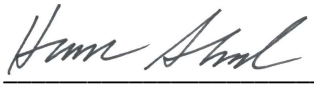
3.4 EXCEPTIONS

Requests for exceptions to this policy may be made by program or department directors (or above) to the Liberty ISO. Exceptions may be granted if access to restricted services is required as part of any current or planned job requirements and/or contractual obligations, with the establishment of appropriate controls and training.

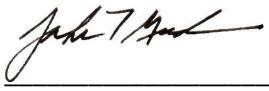
3.5 ENFORCEMENT

Any employee found to be non-compliant and to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Refer to Liberty HIPAA SOP #3 – Complaints, Sanction, and Non-Retaliation for more information regarding the company's enforcement policies.

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 training requirements, email use, and limiting use of third-party services.