Liberty Healthcare Corporation and Affiliates (Liberty) Standard Operating Policies

Title:	**ISF 2.0 – Data 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

2.0 DATA MANAGEMENT POLICY

2.1 PURPOSE

The purpose of the Liberty Healthcare Corporation Data Management policy is to define guidelines to properly classify different types of data managed within the company. This policy also sets various requirements on storage and handling requirements for sensitive data.

All employees should be familiar with the guidelines surrounding the handling of any sensitive data to which they have authorized access.

2.2 SCOPE

The Data Management Policy applies to all applicable data within Liberty Healthcare Corporation and its affiliates (Liberty) including all programs and contracts. Data within these guidelines refers to, but are not limited to, electronic data, physical records, representations of data on paper, or data shared orally or visually.

2.3 POLICY

2.3.1 DATA CLASSIFICATION

All Liberty data are categorized into two main classifications and a few additional subclassifications as become necessary.

1) Liberty Public
2) Liberty Confidential
    a. PHI (Protected Health Information)

Liberty Public information is information or data that have been declared public knowledge with prior authorization by an appropriate party. Information or data in the Liberty Public classification have been deemed appropriate to be shared outside of Liberty without potential damage to the company.

Liberty Confidential contains all other information deemed critical in some manner to the success of the company. All individuals authorized to handle confidential information must understand this information is determined to be sensitive and must be protected and controlled as such. Liberty Confidential information consists of a wide variety of data used in various aspects of the company. This includes, but are not limited to, trade secrets, business development plans, contracts, agreements, financial information, marketing plans, employee information, etc.

Protected Health Information (PHI) is a special subset of Liberty Confidential information. PHI refers to any information regarding any individual's health as defined by the HIPAA Privacy Rule, including but not limited to, participant information, insurance information, medical history, diagnosis, insurance information, enrollment participation, doctor information, etc. The protection requirements of PHI data apply to any data stored, maintained, accessed, or viewed within the Liberty network or facilities, as well as within the networks and facilities of any clients, customers, or affiliated third parties. Any dissemination of PHI data must be authorized by an appropriate party.

2.3.2 DATA CONFIDENTIALITY

All data that is deemed as Liberty Confidential, as well as any subcategories, must be managed and maintained in a secure manner. Confidentiality of the data must be maintained throughout the lifespan of the data; from initial data creation to, and including, the disposal of the data.

2.3.2.1 Least Privilege

Access to all Liberty Confidential Data must be limited to only authorized individuals following the concept of "least privilege." No employees, contractors, or any third parties should have permissions to access any data that are not explicitly required to perform their job functions.

2.3.2.2 Clean Desk

Any individuals working with Liberty Confidential Data must adhere to the clean desk requirements. All Liberty Confidential data must be stored securely and out of sight when not in use. This includes all confidential data on paper as well as that which is stored digitally on workstations or other devices. Physical documents with confidential data must be placed out of site, within locked cabinets, and/or locked offices. Confidential information available on digital devices must not be visible when not in use or away from the location. For example, workstations, mobile devices and any other digital devices must be locked, logged off, or shut down when not in use, requiring a password to re-enter the system to view the information.

Additionally, communal devices such as office printers, scanners, etc. must have all confidential documents removed immediately after use to prevent any possible unauthorized disclosure of confidential information.

2.3.2.3 Asset Management

All assets that access or store any Liberty Confidential information must be traceable with appropriate documentation of asset ownership. This information should be updated regularly as changes occur. This includes information assets such as workstations, servers, storage devices, etc. as well as removable media such as CDs, USB drives, tapes, etc.

Physical paper documents containing Liberty Confidential Information must also be controlled and tracked in reasonable manner.

2.3.3 Encryption Requirements

Wherever possible, all data in transmission and at rest should utilize encryption technologies and protocols to ensure confidentiality and integrity of the data. Liberty Technology Solutions utilize a minimum of AES 128-bit encryption requirement for all secure communication and storage of confidential information. AES-256 is recommended for whenever possible.

2.3.4 Data Backup

All Liberty data must have a viable backup copy saved in an appropriate manner. Data backed up must also adhere to the availability requirements the various contractual and regulatory obligations defined for each individual Liberty program.

All Liberty Confidential data must be encrypted at rest as well as in transit, following the minimum encryption requirements, to maintain confidentiality and security of the sensitive information.

An annual restoration test of the data backup procedures must be completed. Each individual backup process and/or service must complete a restoration test with appropriate verification to ensure the restored data is fully usable. Additionally, the details of each data backup restoration test must be appropriately tracked, recorded, and detailed within a tracking system or ticketing system.

2.3.5 Data Retention

Each individual Liberty program must strictly adhere to the data retention requirements set by contractual and/or regulatory obligations. Please refer to SOP #15 Record Retention and Destruction for specific data retention schedule requirements, unless specifically informed otherwise through contracts, regulations, and any subsequent changes.

When applicable, information system generated logged data must be retained for a minimum of 1 year.

2.3.6 Data Disposal & Reuse

a) Liberty Technology Solutions personnel will work with the program directors, data owners, and the Information Security Officer to verify all instances, locations, and/or backups of the data in question. Logical disposal of the data will include proper wiping of electronic storage devices utilizing an overwrite procedure modeled after the U.S. Department of Defense 5220.22-M Standard. Physical data, paper, tapes, CDs, and other forms of sensitive data should be shredded. Hard drives, solid state drives, flash drives, and other logical storage media that may be found in an array of devices such as workstations, servers, printers, scanners, network devices, mobile devices that have utilized potentially confidential data, must be wiped, degaussed, and/or physically destroyed.

b) Leased computer equipment and hardware including copiers, fax machines, scanners, or any other devices identified to utilize internal storage media, should not be returned to the vendor without appropriate sanitization procedures performed for any embedded media. A review of these devices related data disposal procedures must be performed by the Information Security Officer and, as deemed appropriate, sufficient wipe procedures must be performed prior to returning the device, or any embedded media must be removed prior to return.

c) Vendors utilized and contracted by Liberty to perform media destruction must be a Business Associate, as defined within the HIPAA regulations. The vendor must provide verification of destruction tracking capabilities and provide receipts or other identifying information such as serial numbers, counts, and weight for all associated media.

d) In the event a request for data disposal is received, Liberty Technology Solutions will perform the function with the appropriate authorization from the data owner, program Director, Information Security Officer, and/or the Chief Information Officer. Each disposal request and action must be recorded and tracked within a ticketing system. All disposed

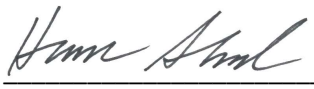
hardware must be tracked appropriately with relevant information documented as applicable, such as count, media type, program information, serial number, make, model, and any other identifying information.

e) In specific situations, the Information Security Officer may authorize the reuse of a storage media device. In this instance, the device must be successfully wiped and sanitized of all potential data in accordance with the U.S. Department of Defense 5220.22-M Standard with an overwrite across all sectors. Any reused storage media must be reimaged and re-encrypted before use. This process and approval must be tracked and documented by the Information Security Officer.

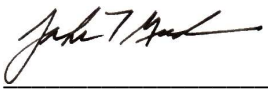
f) Any device or storage media that fails the logical wipe procedure must be fully destroyed to ensure no Liberty Confidential data has the potential to be disclosed.

g) Legacy equipment no longer useful at Liberty that is recognized to retain some value, may be sold or donated accordingly. For all devices set to be sold or donated, all associated long term electronic storage media must be wiped and destroyed according to company standards. Exceptions can only be made with the approval of the Information Security Officer after considering factors such as the original use of the system and potential risk of confidential data exposure.

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 data retention.