National Jewish Health® Science Transforming Life®	Institutional Policy	
	Policy Name	Data Classification, Handling and Disposal
	Effective Date	02/16/2016
	Approved Date	10/15/2018
	Next Approval Date	10/1/2021
	Policy Owner	Judy McCarthy
Approved by: Lazlo Pook, Alicia Christensen		

1. POLICY STATEMENT

This policy establishes the parameters to define the classification of data at National Jewish Health. Non-public data that is collected, processed, stored and transported must be managed and disposed of properly. NJH personnel shall perform these actions and train staff on the procedures. In addition to protecting non-public information, departments shall comply with all federal and state privacy and data security regulations, as well as contractual obligations to protect information.

2. SCOPE

All employees, affiliates, volunteers, and contract employees of National Jewish Health (hereafter referred to as "staff").

3. DEFINITIONS

3.1. Data Owner – the individual ultimately responsible for the data in question. This could be a manager, physician, system administrator, researcher, or staff member.

3.2. Mobile Computing Devices – Laptop computers, tablet computers, cell phones, smart phones, PDA's, and cloud computing.

3.3. Mobile Storage Devices / Removable Media – includes flash memory (thumb) drives, memory sticks, zip/floppy drives, CD's, DVD's, cloud storage, tape drives, or any other portable electronic data storage device.

3.4. IST Help Desk – The IST help desk is available 24 x 7, and can be reached at x1666 or ISHelpDesk@NJHealth.org.

3.5. IS_Central – the online ticketing system used by the IST Help Desk to track and manage service and assistance requests. (https://otrs.njrc.org/forms/ISC-UsersGuide.pdf)

3.6. PHI – Protected Health Information (For a list of what information constitutes PHI see the NJH Confidential Information Agreement.)

3.7. PCI data – Payment Card Industry related data which is includes the primary account numbers (PAN) in combination with other data such as cardholder name, account expiration date, service code, magnetic stripe data, CAV2/CVC2/CVV2/CID, or PINs/PIN blocks.

3.8. PII – Personally Identifiable Information. Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. Further, CO Revised Statutes 6-1-716 defines "personal information" as a Colorado resident's first name or or first initial and last name in combination with one or more of the following data elements that relate to the resident, when the data elements are not encrypted, redacted, or secured by any other method rendering the name or the element unreadable or unusable; Social Security number; student, military, or passport identification number; driver's license number or identification card number; medical information; health insurance identification number; or biometric data; a Colorado resident username or email address, in combination with a password or security question and answers, that would permit access to an online account; or a Colorado resident's account number or credit or debit card number in combination with any required security code, access code or password that would permit access to that account. Protected personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.

4. REQUIREMENTS

4.1 Data Classification

4.1.1 Data shall be classified into the following four levels, according to potential impact:

Unrestricted: Information that would have no measurable impact on NJH in the event of a breach of confidentiality, loss of integrity, or lack of availability.

Examples: Publically available or published information

Level 1: Information that would have little impact on NJH in the event of a breach of confidentiality, loss of integrity, or lack of availability.

Examples: Non-patient related business communications.

Level 2: Information that would have significant financial or operational impact on NJH in the event of a breach of confidentiality, loss of integrity, or lack of availability.

Examples: Non-public financial records, sensitive business plans, sensitive research data or trade secrets, detailed technical information regarding NJH networks/systems/applications, passwords.

Level 3: Information that is required by federal, state, or local law to be protected, or, in the event of breach of confidentiality, loss of integrity, or lack of availability would have serious impact to NJH up to and including physical harm to individuals, or that which would cause significant hardship to NJH, its patients, or the organizations that have entrusted its data to NJH.

Examples: Personnel records, PHI, PCI related data, PII, confidential legal findings, and other confidential records.

4.1.2 It is the responsibility of the data owner to determine appropriate classification levels of the data entrusted to them and to ensure appropriate levels of protection are in place for that data.

4.2 Data Handling

4.2.1 Data Transmission HIPAA 312(a)(2)(iv),312(e)(1),312(e)(2)(ii)

4.2.1.1 NJH shall implement approved methods of transmission for each data type. These methods are outlined in the following minimum requirements table:

Data Type		Electronic Transmission
Unrestricted	NC	No requirement
Level 1		No requirement
Level 2	CONFIDENTIAL	Data may only be transmitted outside of the NJH network when protected by a password or an approved encryption solution.
Level 3		Data must only be transmitted outside the NJH network when protected by an approved encryption solution. Note: PHI data shall not be transmitted outside the NJH network without approval from the NJH Privacy Officer. Note: PHI data shall not be made available to non-NJH personnel without a signed Business Associates Agreement (BAA) or Confidential Information Agreement, whichever is appropriate. HIPAA 164.308(b)(1)

4.2.1.2 Approved Transmission Encryption Methods

4.2.1.2.1 See the NJH Transmission Security Technical Safeguard policy.

4.2.2 Data Storage

4.2.2.1 NJH shall implement approved methods of storage for each data type. These methods are outlined in the following minimum requirements table:

Data Type		Electronic Storage
Unrestricted	NC	No Requirements
Level 1		No Requirements
Level 2	CONFIDENTIAL	• Encrypted when stored on removable media or on a portable computing device. The data must be encrypted or password protected at all times during physical transport. • Encrypted when stored on systems managed by a vendor performing services for NJH. • Shall not be stored on non-NJH owned removable media or portable computing device without authorization from the CIO or the Security Administrator.

Level 3		• Shall not be stored on non-NJH owned removable media or portable computing device without authorization from the CIO, and for PHI, the Privacy Officer. HIPAA 310(d)(2)(iii), 312(a)(2)(iv)
		• Encrypted when stored on removable media or on a portable computing device. The data must be encrypted at all times during physical transport.
		• Encrypted when stored on NJH non-portable systems (servers, workstations), where feasible.
		• Encrypted when stored on systems managed by a vendor performing services for NJH.
		• Cardholder Data Elements (PCI-DSS)
		  ○ Sensitive authentication data (from the magnetic stripe or chip on credit/charge/debit card) shall not be stored.
		  ○ Primary Account Numbers (PAN) shall be rendered unreadable when stored (hashed, truncated, encrypted, etc.).
		• Enable logging to identify access to Level 3 data and securely-stored logs.

4.2.2.2 <u>Approved Storage Encryption Methods</u>

4.2.2.2.1 See the NJH Transmission Security Technical Safeguard policy.

4.2.2.3 Retention CO Law 6 CCR 1011-1 Chap. 4 Part 8.102(2)(a) and (b)

4.2.2.3.1 PHI records for adults shall be retained for a minimum of ten years.
4.2.2.3.2 PHI records for minors shall be retained for the period of minority plus ten years.
4.2.2.3.3 Personnel records shall be retained for a minimum of seven years.
4.2.2.3.4 Financial records (billing, payroll, etc.) shall be retained for a minimum of seven years.
4.2.2.3.5 Cardholder Data Elements (PCI-DSS):

- Sensitive authentication data (from the magnetic stripe or chip on credit/charge/debit card) shall not be stored.
- Primary Account Numbers (PAN) shall be rendered unreadable when stored (hashed, truncated, encrypted, etc.).

4.2.2.4 Inventory HIPAA 310(d)(1), 310(d)(2)(iii)

4.2.2.4.1 An inventory of all mobile computing devices and mobile storage devices (NJH, vendor, or personally owned) containing Level 3 data shall be maintained by IST.
4.2.2.4.2 All departments must inform IST via IS_Central or the IST Help Desk when a mobile computing or storage device is used to store Level 3 data for the first time.
4.2.2.4.3 Inventory information at a minimum must include the name of the person responsible, the device type (laptop, portable hard drive, cloud storage, etc.), and the general type of Level 3 data stored (PHI, PCI, Personnel data).

4.2.2.5 Integrity

4.2.2.5.1 See the NJH Integrity Technical Safeguard policy.

4.2.2.6 Physical Security

4.2.2.6.1 See the NJH Workstation Security Physical Safeguard policy.

4.2.3 Data Disposal

4.2.3.1 NJH shall implement approved methods of deletion for each data type. These methods are outlined in the following minimum requirements table:

Data Type		Electronic Data Deletion / Destruction
Unrestricted	NC	Standard file deletion, no destruction requirement
Level 1		Standard file deletion, no destruction requirement
Level 2	CONFIDENTIAL	Render data unrecoverable: 1. Utilize an IST approved secure wipe program prior to media re-use, or 2. Destroy/degauss media
Level 3		Render data unrecoverable: HIPAA 310(d)(2)(i), 310(d)(2)(ii), 312(c)(2) 1. Utilize an IST approved secure wipe program prior to media re-use, or 2. Destroy/degauss media 3. A record of disposal shall be maintained

4.2.3.2 Media Re-Use

4.2.3.2.1 IST must remove, i.e. “wipe”, electronic data when repurposing systems containing Level 2 and 3 data. This applies to all mobile computing devices and removable media and includes but is not limited to USB flash memory devices, external USB drives, floppy disks, CD and DVD re-writable disks, Blu-ray re-writable disks, cellphones, Black Berries or other PDA type devices, printers, copy machines, or scanners, inclusive of any future removable media technologies and appliances.

4.2.3.2.2 If the highest data classification on a repurposed system is unknown, then it must be wiped prior to re-use.

4.2.3.2.3 Mobile computing devices/storage devices containing Level 2 and 3 data must be securely wiped prior to re-use. This includes NJH and non-NJH owned systems, and also includes such devices during employee separation.

4.2.3.2.4 Cloud computing services hosting NJH Level 2 and 3 data must contractually guarantee that confidential data will be rendered inaccessible (i.e. wiped) upon termination of services.

4.2.3.2.5 See the NJH Device and Media Controls Physical Safeguard policy.

4.2.3.3 Media Disposal – Level 2 and 3 Data

4.2.3.3.1 Removable media containing Level 2 or 3 data must be securely wiped or physically destroyed when disposed of.

4.2.3.3.2 Mobile device hard drives and non-volatile memory components must be securely wiped or physically destroyed when disposed of.

4.2.3.3.3 Media shall be physically secured between the time it is identified for data destruction/removed from its device and the time when data is destroyed.

4.2.3.3.4 Media destruction must be performed by a licensed or certified data destruction business.

4.2.3.3.5 See the NJH Device and Media Controls Physical Safeguard policy.

4.2.3.4 Hardcopy Disposal – Level 2 and 3

4.2.3.4.1 Paper must be physically destroyed prior to disposal (burned or cross-cut shredded).
4.2.3.4.2 Film, microfiche, etc. must be burned and reduced to white ash prior to disposal.
4.2.3.4.3 These items may also be placed in the secure document disposal containers located on NJH property for secured disposal.

4.2.3.5 Disposal Record (Level 3)

4.2.3.5.1 All electronic media containing Level 3 data that is securely wiped, degaussed or destroyed shall have a disposal record created.
4.2.3.5.2 Upon data/media destruction the device owner must inform IST so the mobile device inventory may be updated and a data/media disposal record can be created.
4.2.3.5.3 The disposal record shall, at a minimum, record the media description, identification (serial number, inventory number, etc.), department data owner, date and time of data/media destruction, and person performing the destruction.

5. ROLES AND RESPONSIBILITIES

5.1. Department Director - is responsible for designating and approving system owners, data owners, and system administrators for all major applications and critical systems.

5.2. Chief Information Officer (CIO) - is responsible for:
- Ensuring the requirements of this policy are integrated into National Jewish Health system procedures.
- Ensuring that all legacy systems that cannot meet this policy are retired or upgraded.

5.3 EPHI Security Team - is responsible for assuring ongoing monitoring and auditing the effectiveness of this policy.

5.4 Data Owner – the individual ultimately responsible for the data in question. Responsible for correctly classifying data and for ensuring appropriate methods of protection are followed.

5.5 System Owner/Manager - is responsible for ensuring data on their system is properly classified and protected.

5.6 IT Staff - are responsible for implementing data classification, handling, and disposal procedures that prevent unauthorized access to NJH information.

5.7 End User - is responsible for following data classification, handling, and disposal procedures that prevent unauthorized access to NJH information.

5.8 Information Services and Technology (IST) - responsible for implementing solutions that protect data in transmission and at rest appropriate to its level, and to appropriately dispose of data and media.

5.9 IST Help Desk – is responsible for being the main point of contact to NJH for IT related issues and IST services.

6. REFERENCES

6.1. FIPS 199, Standards for Security Categorization of Federal Information and Information Systems

6.2. HIPAA Security Rule 164.308(b)(1), 310(d)(1), 310(d)(2)(i), 310(d)(2)(ii), 310(d)(2)(iii), 312(a)(2)(iv), 312(b), 312(c)(1), 312(c)(2), 312(e)(1),312(e)(2)(ii)

6.3. NIST SP 800-53r3, Recommended Security Controls for Federal Information Systems and Organizations

6.4. NIST SP 800-88, Guidelines for Media Sanitization

6.5. NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information.

6.6. Payment Card Industry Data Security Standard (PCI DSS) Requirements 3.1 (3.1.1), 3.2 (3.2.1-3), 3.3, 3.4, 3.5, 3.6, 4.1 (4.1.1), 4.2, 9.5, 9.6, 9.7 (9.7.1-2), 9.8, 9.9 (9.9.1), 9.10 (9.10.1-2)

6.7. State of Colorado Record Retention Schedules: 6 CCR 1011-1 Chap. 4 Part 8.102(2)(a) and (b)

6.8. State of Colorado Protections for Consumer Data Privacy Regulation – CRS 6-1-713, 6-1-716, and 24-73-101.

REVIEWED BY: Liam Schneider