Data Destruction

1

Overview

- Recent enforcement action for improper disposal of tangible PHI and paper records
- On-going concerns about destruction of PHI and ePHI
- Operational Costs
- Overview of Legal Landscape
- Data Retention guidelines
- Best Practice Standards for Destruction

2

New England Dermatology and Laser Center (NEDLC)

Empty labeled (PHI) specimen containers were placed in a dumpster in the parking lot

PHI included patient name, date of birth, date of sample collection, and name of provider who took the specimen

One specimen container bearing a label with PHI was found in the parking lot by a third-party security guard

3

New England Dermatology and Laser Center

Standard practice – regularly discarded specimen containers with an attached label that contains PHI as regular waste

Regular waste is bagged and place in the dumpster in parking lot without alteration to PHI on the label

February 4, 2011 – March 31, 2021

More than 10 years!

4

New England Dermatology and Laser Center

Data Breach Notification Report to OCR on May 11, 2021

Resolution Agreement in July 2022

Violated:

- 45 CFR §164.530(c) – Administrative Requirements
  - *Standard: Safeguards – A CE must have in place appropriate administrative, technical and physician safeguards to protect the privacy of PHI*
- 45 CFR §164.502(a) – Uses and Disclosures of PHI
  - *Standard: A CE or BA may not use or disclose PHI except as permitted or required by the rule*

Basic HIPAA Privacy Rule requirements

5

NEDLC Resolution Agreement

Resolution amount of $300,640

2-year term

Corrective Action Plan ("CAP") – 60, 90, 120-day OCR deadlines

- Policies and Procedures (P&Ps)– all HIPAA Privacy Rule
- Distribution and Updating of P&Ps
- Training – within 60 days
- Reportable Events – failure of workforce members and business associates and notification to OCR within 30 days
- Implementation Report – within 120 days, with attestations
- Annual Report – compliance with CAP
  - Training materials, attestations, summary and status of Reportable Events
- Document Retention – 6 years
- Breach Provisions – Civil Monetary Penalties ("CMP")

6

CVS Caremark

Pharmacies throwing trash into open dumpsters that contained pill bottles with:

- patient names
- addresses
- prescribing physicians' names
- medication and dosages
- medication instruction sheets with personal information
- computer order information from pharmacies with customer PHI

Also:

- Employment applications, including social security numbers, payroll info, credit card and insurance card info, account numbers and driver's license numbers

7

CVS Caremark

- Media reports from around the country reported violations

- Variety of violations from April 2003 – May 2007
  - Improper disposal of non-electric PHI accessible to unauthorized workforce
  - P&Ps related to physical and administrative safeguards were **ineffective**
  - Lack of a sanctions policy for workforce members
  - Training was **not sufficient** to ensure proper disposal of non-ePHI

8

CVS Resolution Agreement

- January 2009
- 3 year term
- $2.25 million civil penalty
- Corrective Action Plan ("CAP")

- Coinciding FTC investigation – ordered implementation of information security program and external third-party audit every 2 years for next 20 years

9

Why is this important? Operational Costs

- Cost of data breaches
  - "The average breach in healthcare increased by nearly USD 1 million to reach USD 10.10 million. Healthcare breach costs have been the most expensive industry for 12 years running, increasing by 41.6% since the 2020 report." IBM Security Cost of a Data Breach Report 2022

10

Legal Landscape

- HIPAA
- Federal Record Retention Requirements
- State Retention Rules
- State Destruction Rules
- Legal Holds

11

Legal Landscape: HIPAA

- Does not regulate medical retention requirements.
- Requires reasonable safeguards to limit incidental, and avoid prohibited, uses and disclosures of PHI, when disposing PHI.
- Requires policies and procedures to address the final disposition of electronic PHI and removal of PHI from electronic media before it is re-used.
- Requires training of workforce on proper disposal of PHI.

45 CFR 164.530(c)
45 CFR 164.310(d)(2)

12

Legal Landscape: HIPAA

Incidental Uses and Disclosures

- Incidental uses and disclosures are secondary uses or disclosures that cannot reasonably be prevented, are limited in nature, and that occur as a result of another use or disclosure that is permitted by the Rule.
- An incidental use or disclosure is **not** permitted if it is a by-product of an underlying use or disclosure which violates the Privacy Rule (e.g., reasonable safeguards, minimum necessary).
- Failing to implement reasonable safeguards to protect PHI in connection with disposal could result in impermissible disclosures of PHI.

45 CFR 164.502(a)(1)(iii)

13

Legal Landscape: HIPAA

Paper Records:

- Phone messages, faxes, prescription refill slips, medical record request slips, medical reports, etc.
- Shredding, burning, pulping, or pulverizing the records so that PHI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed.

Electronic media:

- Backup tapes, computer hard drives, USB drives, file servers
- Clearing (using software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media (disintegration, pulverization, melting, incinerating, or shredding)

14

Legal Landscape: Federal Record Retention Requirements

Federal record retention requirements may be triggered based on funding

Examples:

- Abortion and related programs or projects for health services which are supported in whole or in part by federal financial assistance appropriated to the Department of Health and Human Services must maintain documentation for three years. 42 CFR § 50.309.
- Certain comprehensive outpatient rehabilitation facilities are required to maintain clinical records for 5 years after patient discharge and must make provision for the maintenance of such records if it is no longer able to treat patients. 42 CFR § 485.60.

15

Legal Landscape: State Retention Rules

May be based on:

- Length of time
  - For example, Alaska, Colorado, Illinois
- Type of provider
  - For example, Texas retention law differs between hospitals and physicians. 22 Tex. Admin. Code 165.1; Tex. Health & Safety Code 241.103.
- Patient Condition or Record Type
  - For example, Mississippi has different retention laws for x-ray films and other graphic data in comparison to other medical records. Miss. Code Ann. 41-9-69.

16

Legal Landscape: State Destruction Rules

States may have specific laws governing how information containing personal data must be destroyed.

For example, Wisconsin. Wisc. Stat. § 134.97

- (2) Disposal of records containing personal information. A financial institution, medical business or tax preparation business may not dispose of a record containing personal information unless the financial institution, medical business, tax preparation business or other person under contract with the financial institution, medical business or tax preparation business does any of the following:
  - (a) Shreds the record before the disposal of the record.
  - (b) Erases the personal information contained in the record before the disposal of the record.
  - (c) Modifies the record to make the personal information unreadable before the disposal of the record.
  - (d) Takes actions that it reasonably believes will ensure that no unauthorized person will have access to the personal information contained in the record for the period between the record's disposal and the record's destruction.

17

Legal Landscape: State of Wisconsin: Administrative Code

Wis. Admin. Code MED §21.03 ("A physician or physician assistant shall maintain patient health care records on every patient administered to for a period of not less than 5 years after the date of the last entry, or for such longer period as may be otherwise required by law.")

Wis. Admin. Code DHS §133.21 (home health)("An original medical record and legible copy or copies of court orders or other documents, if any, authorizing another person to speak or act on behalf of this resident shall be retained for a period of at least 5 years following a resident's discharge or death when there is no requirement in state law. All other records required by this chapter shall be retained for a period of at least 2 years.")

Wis. Admin. Code DHS §131.33 (hospices) ("An original clinical record and legible copy or copies of court orders or other documents, if any, authorizing another person to speak or act on behalf of the patient shall be retained for a period of at least 5 years following a patient's discharge or death when there is no requirement in state law. All other records required by this chapter shall be retained for a period of at least 2 years.")

Wis. Admin. Code DHS §132.45 (nursing homes) ("An original medical record and legible copy or copies of court orders or other documents, if any, authorizing another person to speak or act on behalf of this resident shall be retained for a period of at least 5 years following a resident's discharge or death when there is no requirement in state law. All other records required by this chapter shall be retained for a period of at least 2 years.")

Wis. Admin. Code DHS § 88.09 (licensed adult family homes) ("The licensee shall retain a resident's record for at least 7 years after the resident's discharge. The record shall be kept in a secure, dry place."

Wis. Admin. Code DHS §92.12 (substance abuse) (" Treatment records shall be retained for at least 7 years after treatment has been completed, unless under this section they are to be retained for a longer period of time. In the case of a minor, records shall be retained until the person becomes 19 years of age or until 7 years after treatment has been completed, whichever is longer.")

18

Legal Landscape: Legal Holds

1. A legal hold (also known as a litigation hold) is a notification sent from an organization's legal team to employees instructing them not to delete electronically stored information (ESI) or discard paper documents that may be relevant to a new or imminent legal case.
2. Send when litigation commences or can be reasonably anticipated
3. Send to anyone who might possess potentially relevant information
4. Describe the specific electronic data or paper documents that need to be preserved: Describe name, dates, underlying matter.
5. Track acknowledgments of the hold; remind custodians of their hold obligations; suspend auto-deletion.

19

What can you do next?

- Best Practices for Destroying Data
- Inventory
- Data Retention Schedules
- Workforce Training and Policies and Procedures

20

What can you do next? Inventory

Identify what PHI you have and create

Identify where that PHI resides or is created in your organization
- Paper Records
- Mobile devices
- Cloud based applications

Identify what PHI resides with or is created by vendors

Identify what PHI is subject to other controls such as a legal hold or an investigation

Regularly update the data inventory

21

What can you do next? Data Retention Schedules

Goal of Data Retention Schedule is to determine which content has value beyond its original purpose or otherwise must be retained pursuant to law

- Create an inventory of data and create categories (e.g., medical records, x-rays, etc.)
- Determine which regulations, policies, laws apply to each category of data
- Determine how long information should be archived and when it should be deleted
- Determine how the information should be deleted
- Determine where official records should be kept and by whom
- Draft a policy and train workforce members

22

What can you do next? Training and Policies and Procedures

Identification of what PHI is

Identification of where PHI can be found

Training on how to dispose of PHI and when to dispose of PHI
- Location of shredders
- Return of media devices / notification of lost media devices

Paper record considerations
- Will you have restrictions on printing and copying PHI?
- Will you have shredders / opaque bags on site?

Electronic media considerations
- What electronic media will you permit?
- Under what circumstances will you permit the re-use of electronic media, internally and externally?
- What electronic media sanitation guidelines will you require?
- How will you ensure that employee electronic media is returned and wiped?

23

Considerations for Remote Workforce

Before pandemic - 24% American workforce worked from home 3-5 days/week

After pandemic - 53% American workforce words from home 3-5 days/week*

Move to remote workforce happened very rapidly!

HIPAA Rules are applicable no matter where your PHI is
- **45 CFR §164.530(c)** – *appropriate administrative, technical and physician safeguards to protect the privacy of PHI*
- **45 CFR §164.502(a)** – Uses and Disclosures of PHI still governed by HIPAA

*Remote work frequency before/after COVID-19 2020 | Statista

24

Considerations for Remote Workforce

Significant financial penalties for failure to properly protect PHI

Access, retention, and destruction policy decisions should be reviewed

Access Considerations
- Unauthorized access by family, friends, etc.
- VPNs, encryption, multi-factor identification
- Define equipment, software, hardware requirements

Ability to print and dispose of paper – shredding requirements

25

Considerations for Remote Workforce

Is your remote workforce captured on your Security Risk Assessment (SRA)?
- Risks and vulnerabilities
- Required when there is a significant change to your business practices

What about your vendors/Business Associates remote workforce?
- Where is your PHI being retained and disposed of?

Evaluate your current policies and procedures

Remote Access Agreement – capture security requirements
- Access, retention, and disposal

26

What can you do next? Vendor Agreements and Vendor Management

Considerations when drafting vendor agreements
- Is the vendor maintaining the official records? (E.g., are they holding the source of truth?)
- How will you enforce the return or destruction of data at the end of an agreement?
  - Certifications of destruction?
  - Contracted timelines for return or destruction of data?
  - Terms regarding format of data?
- Is the data segregated from other client's data?
- Auditing Rights

27

Best Practice Standard for Destruction

Neither the Privacy or Security Rules dictate a particular method of disposal

U.S. Department of Commerce - **National Institute of Standards and Technology (NIST)**
- Non-regulatory agency whose mission is to promote American innovation and industrial competitiveness, including Information Technology

NIST Special **Publication 800-88**, Revision 1, December 2014, "Guidelines for Media Sanitization."
- National and international standard for "**sanitization**" standards

Addresses sanitization of all/every type of media, *even those yet to be invented*

28

Best Practice Standard for Destruction

- The determination of how to destroy or dispose of data is based on the level of sensitivity of the data itself (not necessarily the media on which the data is stored)
- Type and level of sensitivity of data determines necessary level of destruction or "Sanitization"

29

Sanitization

Sanitize means "a process to render access to target data on the media infeasible for a given level of effort."

- **Clear** – applies logical techniques to sanitize data in all user-addressable storage locations and protects against simple, non-invasive data recovery techniques; **moderate level of data protection**
- **Purge** – applies physical or logical techniques that render target data recovery infeasible using state-of-the-art lab techniques; more thorough level of sanitization; more confidential data protection
- **Destroy** – renders target data recovery infeasible using state-of-the-art lab techniques that **renders the media incapable of storing data afterward**; shredding, incinerating, pulverizing, melting, or other physician techniques.

30

Best Practice Standard for Destruction

Hard Copy Storage - Paper and microforms (microfilm, microfiche, or other reduced image photo negatives

Table A-1: Hard Copy Storage Sanitization

Hard Copy Storage	
Paper and microforms	
Clear:	N/A, see Destroy.
Purge:	N/A, see Destroy
Destroy:	Destroy paper using cross cut shredders which produce particles that are 1 mm x 5 mm (0.04 in. x 0.2 in.) in size (or smaller), or pulverize/disintegrate paper materials using disintegrator devices equipped with a 3/32 in. (2.4 mm) security screen. Destroy microforms (microfilm, microfiche, or other reduced image photo negatives) by burning.
Notes:	When material is burned, residue must be reduced to white ash.

31

Medical Record Request

32

HIPAA Security – Device and Media Controls

§ 164.310 - Physical safeguards.

A covered entity or business associate must, in accordance with § 164.306:

- **(d)(1)** ***Standard:*** ***Device and media controls. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.***
- ***(2) Implementation specifications:***
- **(i)** ***Disposal (Required).*** **Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.**
- (ii) ***Media re-use (Required)***. Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.
- (iii) ***Accountability (Addressable).*** Maintain a record of the movements of hardware and electronic media and any person responsible therefore.
- (iv) *Data backup and storage (Addressable).* Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

33

Best Practice Standard for Destruction

Optical Media – CD, DVD, BD

Table A-6: Peripherally Attached Storage Sanitization

Peripherally Attached Storage	
External Locally Attached Hard Drives (Thunderbolt, USB, Firewire, etc. (SAS/SATA/ATA/PATA/IDE/EIDE))	
Clear:	Overwrite media by using organizationally approved and tested overwriting technologies/methods/tools. The Clear pattern should be at least a single pass with a fixed data value, such as all ones. Multiple passes or more complex values may alternatively be used.
Purge:	The implementation of External Locally Attached Hard Drives varies sufficiently across models and vendors that the use/areas of any specific command to the device may not reasonably and consistently assure the desired sanitization result. When the external drive bay contains an ATA or SCSI hard drive, if the commands can be delivered natively to the device, the device may be sanitized based on the associated media-specific guidance. However, the drive could be configured in a vendor-specific manner that precludes sanitization when removed from the enclosure. Additionally, if sanitization techniques are applied, the hard drive may not work as expected when reinstalled in the enclosure. Refer to the device manufacturer to identify whether the device has a Purge capability that applies media-standard techniques (such as overlap, block erasing, Cryptographic Erase, etc.) to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Verification as described in the Verify Methods subsection must be performed for each technique within Clear and Purge. Some external locally attached hard drives, especially those featuring security or encryption

34

Contact Info

Allison Dressel
Polsinelli
adressel@polsinelli.com
312.463.6355

Kirsten Ruzic Wild, BSN, MBA, CHC
Wild Consulting, Inc.
kirsten@wildconsultinginc.net
262.993.4747

35