Training Session Handouts

Avoid Medical Record Destruction Mistakes and the $50,000 Fine

Presented by:
Daphne Kackloudis, Esq. and Ashley Watson, Esq.

HEALTHCARE TRAINING LEADER®
Expert Medical Practice Solutions

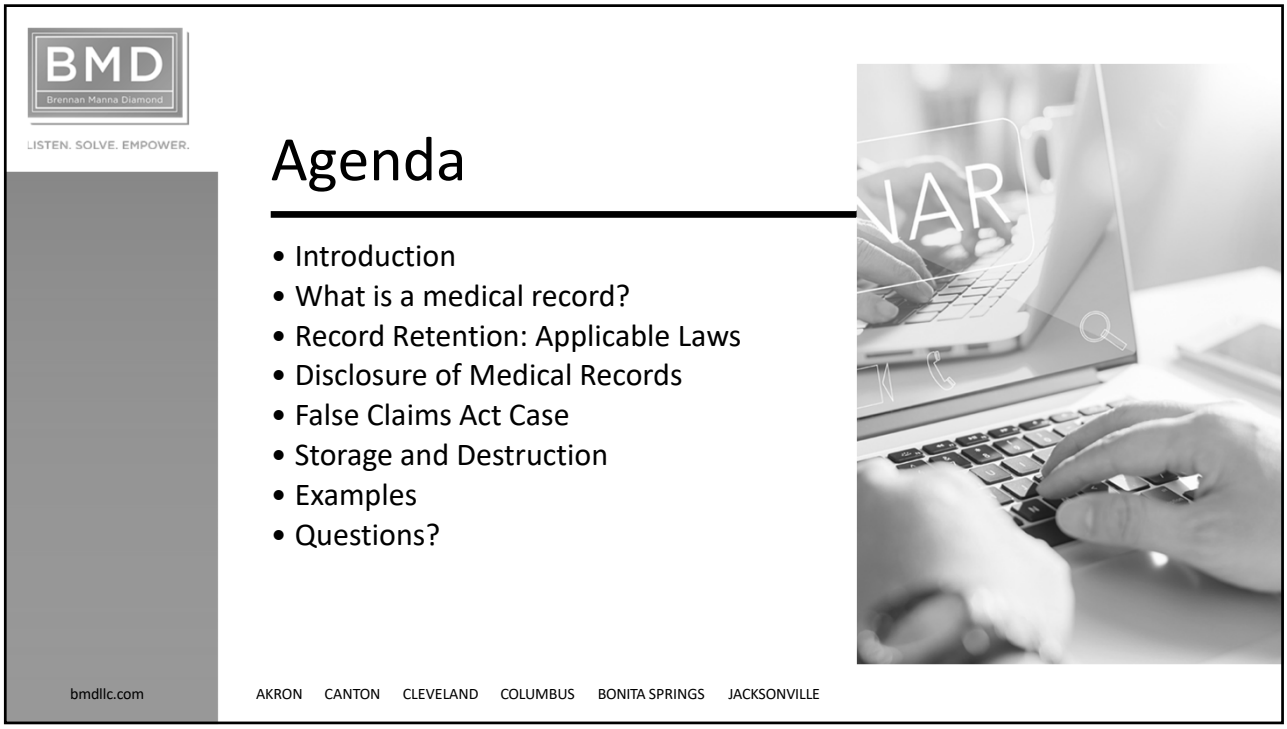
[DISCLAIMER]
© Training Leader. This 2021 Webinar Handout is published by Healthcare Training Leader, a division of Must Have Info, Inc. Reproduction or further distribution by any means, beyond the paid customer, is strictly forbidden without written consent of Training Leader, including photocopying and digital, electronic, and/or Web distribution, dissemination, storage, or retrieval.

This webinar is an independent product of Healthcare Training Leader. It is not endorsed by nor has it any official connection with any other organization, insurance carrier, vendor, or company. Reasonable attempts have been made to provide accuracy in the content. However, of necessity, examples cited and advice given in a national periodical such as this must be general in nature and may not apply to any particular case. The publisher, editors, board members, contributors, nor consultants warrant or guarantee that the information contained herein on coding or compliance will be applicable or appropriate in any particular situation.

(c) 2021 Must Have Info, Inc. All Rights Reserved.
Healthcare Training Leader®, 2277 Trade Center Way,
Suite 101, Naples, FL 34109, Phone: 800-767-1181 •
Fax: 800-767-9706 • E-mail: info@trainingleader.com •
Website: www.hctrainingleader.com

BMD
Brennan Manna Diamond
LISTEN. SOLVE. EMPOWER.
Medical Record Destruction Best Practices
Training Leader Webinar
Daphne L. Kackloudis, Partner
Ashley B. Watson, Associate
bmdllc.com
AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

1


BMD
Brennan Manna Diamond
LISTEN. SOLVE. EMPOWER.
Agenda
• Introduction
• What is a medical record?
• Record Retention: Applicable Laws
• Disclosure of Medical Records
• False Claims Act Case
• Storage and Destruction
• Examples
• Questions?
bmdllc.com
AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

2

BMD
Brennan Manna Diamond
LISTEN. SOLVE. EMPOWER.

Introduction

- Who are we?
- What is BMD?

bmdllc.com

AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

3

BMD
Brennan Manna Diamond
LISTEN. SOLVE. EMPOWER.

What is a Medical Record?

bmdllc.com

AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

4

BMD
Brennan Manna Diamond
LISTEN. SOLVE. EMPOWER.

Medical Records

- Medical records or health records can consist of a variety of documents.
  - Physician records
  - Pharmacy records
  - Psychiatrist records
  - Diagnostics
  - Administrative and financial data
  - Etc.
- *Griffith v. Aultman Hosp.*, Slip Opinion No. 2016-Ohio-1138

bmdllc.com AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

5

BMD
Brennan Manna Diamond
LISTEN. SOLVE. EMPOWER.

Medical Records

- Health records can be stored on:
  - Paper
  - Video
  - Audio files
  - Images
  - E-mail
- Information is often stored in multiple systems, making it difficult to pull someone's entire health record or designated record set.
- Documentation in the medical record provides evidence of appropriate care. Having proper documentation is the minimum needed to show that a procedure was completed.

bmdllc.com AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

6

Defining the Record

- All practices should develop a written policy defining the legal health record and the designated record set and identifying where the records physically exist.
- The primary consideration in defining the legal health record and designated record set must always be the needs for immediate and long-term patient care.
- A health information committee comprised of patient care team members and administrative staff can guide this process. Members of this committee should make the decision on what information is clinically meaningful.
- Suggested steps:
  - Identify relevant regulations, standards, and laws
  - Determine records created in the course of business
  - Address retention requirements
  - Consider how data would be produced
  - Classify external records
  - Review regularly

bmdllc.com

AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

7

Record Retention

bmdllc.com

AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

8

BMD
Brennan Manna Diamond
LISTEN. SOLVE. EMPOWER.

Retention

- Records must be retained in a way that is secure and makes retrieval by the provider as easy as possible.
- All practices should have a record retention schedule to help them follow relevant laws.
- At a minimum, record retention schedules must:
  - Ensure patient health information is available to meet the needs of continued patient care, legal requirements, research, education, and other legitimate uses of the organization.
  - Include guidelines that specify what information is kept, the time period for which it is kept, and the storage medium on which it will be maintained (e.g., paper, microfilm, optical disk, magnetic tape).
  - Include clear destruction policies and procedures that include appropriate methods of destruction for each medium on which information is maintained.

bmdllc.com

AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

9

BMD
Brennan Manna Diamond
LISTEN. SOLVE. EMPOWER.

Type of Record	Minimum Retention Period by Law	Recommended Retention Period
Patient Medical Records		
Services rendered by licensed* : ▪ clinics ▪ health facilities ▪ adult day health care centers ▪ home health agencies * such entities must preserve patient records even after the licensee ceases operations.	7 years following patient discharge	10 years
▪ Services reimbursed by Emergency Services Funds ▪ Schedule II drug dispensing and prescribing records	3 years	5 years
Medi-Cal Patients	10 years	10 years
HMO Health Plans subject to Knox Keene Act	3 years	5 years
Medical records for Workman's Compensation evaluations	5 years	5 years

bmdllc.com

AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

10

LISTEN. SOLVE. EMPOWER.

Federal Laws, HIPAA

- Health Insurance Portability and Accountability Act (HIPAA) of 1996
  - 45 CFR 164.316
- Requires a covered entity to retain required documentation for six (6) years from the date of its creation or the date when it last was in effect, whichever is later.
- HIPAA requirements preempt State laws if they require shorter periods.
- The medical record needs to be in its original form or in a legally reproduced form, which may be electronic, so that medical records may be reviewed and audited by authorized entities.
- Providers must have a medical record system that ensures that the record may be accessed and retrieved promptly.

bmdllc.com

AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

11

LISTEN. SOLVE. EMPOWER.

State Laws

- Most states have medical record retention laws that range from 5-10 years
- Note requirements for individual practitioners vs. institutions
- Also note requirements for minors
  - Must retain records past the age of majority, usually until the patient is between 23 and 28.
- Also look at statutes of limitations for medical malpractice claims and worker's compensation claims for your state

bmdllc.com

AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

12

Retention

- Record retention guidelines should follow the most restrictive requirement considering:
  - State law;
  - False Claims Act (31 USC 3729) – claims may be brought up to ten years after the incident (recently updated – more to come!);
  - Accreditation requirements (Ex: Medicare Conditions of Participation, Joint Commission);
  - Special populations may be governed by other regulations: minors, behavioral health, or research patients.
    - The Food and Drug Administration, for example, requires research records pertaining to cancer patients be maintained for 30 years.
    - The CDC requires health care providers who administer certain vaccines to ensure that the permanent medical record of the recipient (or a permanent office log or file) indicates several details about any vaccination. (42 USC 300aa-25(a))

bmdllc.com

AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

13

Example: Hospital Retention Requirements

Federal Requirement	State Requirement	Accreditation Requirement
Hospitals: Five years. Must be able to access both inpatient and outpatient records for this period and promptly retrieve medical records upon request. Conditions of Participation – 42 CFR 482.24(b)(1)	Each health care facility shall maintain medical records as necessary to verify the information and reports required by statute or regulation for at least six years from the date of discharge. OAC 3701-83-11(F)	Joint Commission RC.01.05.01: The hospital retains its medical records. The retention time of the original or legally reproduced medical record is determined by its use and hospital policy, in accordance with law and regulation.

***Remember the False Claims Act too!**

bmdllc.com

AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

14

Disclosure of Medical Records

bmdllc.com

AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

15

Under HIPAA

- Only the patient or their personal representative has the right to access their medical records.
- Individuals have a right to access this PHI for as long as the information is maintained by a covered entity, or by a business associate on behalf of a covered entity, regardless of the date the information was created; whether the information is maintained in paper or electronic systems onsite, remotely, or is archived; or where the PHI originated (e.g., whether the covered entity, another provider, the patient, etc.).
- The patient may direct a health care provider or health plan to send copies of their records to another provider or health plan only as needed for treatment or payment or with their permission.

bmdllc.com

AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

16

Requests for Medical Records

- Make a "request for sending medical records" checklist to use every time:
  - Request to send records should have at least two types of identifiers
  - Where is it going? Address/fax/portal
  - What information actually needs to be sent?
    - Minimum necessary
    - Dates of service
  - Expiration date (1 year unless…)
  - Patient signature and date
    - Patients need to use legal name
- Real life example of denial: patient requesting their record puts today's date instead of DOB
- Keep a good record of when the record was requested and who fulfilled the request
  - Retain in the patient's medical record
- The Privacy Rule permits a covered entity to impose a reasonable, cost-based fee if the individual requests a copy of the PHI

bmdllc.com

AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

17

Request Denials/Corrections

- A request can be denied under limited circumstances:
  - Request for psychotherapy notes or information compiled for a legal proceeding;
  - Information is part of a clinical trial still in progress;
  - Sending information would jeopardize the health and safety of the individual or another person.
- Corrections
  - A patient may request a correction to their medical record if they think it is incorrect.
  - If you are the provider that created the information, you must amend inaccurate or incomplete information.
- Providers have 60 days to respond to a request to correct the medical record.

bmdllc.com

AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

18

State Laws

- Many states have laws or regulations that give individuals the right to their health information.
- Some state laws may define health information more broadly than the privacy rule.
- Some states may not limit access and amendment to PHI in a designated record set.
- When state laws or regulations afford individuals greater rights of access, the covered entity must adhere to state law.

bmdllc.com AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

19

False Claims Act Case Law Update

bmdllc.com AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

20

Cochise Consultancy Inc. v. United States, ex rel. Hunt

- Background:
  - The FCA establishes liability for anyone who improperly receives payments from, or avoids payments to, the Federal Government. Ex:
    - Knowingly presenting, or causing to be presented a false claim for payment or approval;
    - Knowingly making, using, or causing to be made or used, a false record or statement material to a false or fraudulent claim; and
    - Knowingly making, using, or causing to be made or used a false record to avoid, or decrease an obligation to pay or transmit property to the Government.
  - A claim alleging that a provider has violated the FCA can be brought by a private citizen, known as a qui tam or whistleblower action, or by the Federal Government.
  - If a claim is brought by a private citizen, the Federal Government can choose to intervene or choose to stay out of the case and let the private citizen handle the litigation.

bmdllc.com AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

21

Background, cont.

- The FCA has two statutes of limitation. A claim under the FCA may not be brought:
  - more than 6 years after the date when the violation was committed, or
  - more than 3 years after the date when facts material to the case are known or reasonably should have been known by an official of the United States, but in no event more than 10 years after the date when the violation was committed.
- Whichever statute of limitations is longer will apply. In actions where the government intervenes, it is clear that the second statute of limitations applies.
- The question in the *Cochise* case revolves around whether the ten-year statute of limitations can also apply to cases where the government does not intervene, which is a majority of the cases.

bmdllc.com AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

22

The Case

- In the *Cochise* case a private citizen, Hunt, filed a *qui tam* complaint more than six years after the Cochise Consultancy allegedly violated the FCA but less than three years after he informed a government official of the violations, and within the ten-year limitation period.
  - Over first statute of limitations, but within second
- The government chose not to intervene in the lawsuit and Cochise argued that, as a result, only the six-year statute of limitations applied.
- The Supreme Court disagreed, finding that Hunt had filed the case within three years of notifying a government official and less than ten years from the date of the violation.
- Further, the Court clarified that a private citizen in a non-intervened suit is not a government official, so their knowledge does not trigger the three-year limitations period.

bmdllc.com AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

23

The Takeaway: Retain Your Medical Records

- For providers, the Cochise decision means that you may be vulnerable to FCA claims for up to 10 years after an alleged violation.
- Medical records can prove to be a powerful tool in defending against alleged FCA violations. Proper documentation can support medical necessity for claims submitted to Medicare for payment.
  - However, if the medical records no longer exist, a provider's argument against a violation is much weaker.
- Prior to this decision most medical records policies specified that records should be retained for at least six years to be in line with HIPAA guidelines, or longer depending on state law.
- **Now, it is recommended that you revise your medical record retention policies to retain all medical records for at least ten years to better protect yourself and your practice from any possible FCA claims.**

bmdllc.com AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

24

BMD
Brennan Manna Diamond
LISTEN. SOLVE. EMPOWER.

Storage and Destruction

bmdllc.com

AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

25

BMD
Brennan Manna Diamond
LISTEN. SOLVE. EMPOWER.

Storage and Retrieval

- Questions organizations must ask include:
  - What information can, or must, be stored long term?
  - What information is clinically useful long-term?
  - What is the cost of storage?
  - How can the organization effectively and succinctly assemble the EHR for long-term use?
- Tips:
  - If your practice utilizes an EHR or a cloud storage system then all records can be kept within that system
  - Ensure you have the IT knowledge and support to retrieve records as necessary

bmdllc.com

AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

26

BMD
Brennan Manna Diamond
LISTEN. SOLVE. EMPOWER.

Storage Practices

- Storage systems could include:
  - Lockable filing cabinets
  - Storage boxes
  - Rented storage spaces
  - Storage companies
  - Electronic storage
  - CDs
  - Tapes
  - Cloud
- Practices must consider:
  - Space
  - Cost
  - Security
  - Type of records being stored

bmdllc.com AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

27

BMD
Brennan Manna Diamond
LISTEN. SOLVE. EMPOWER.

More on Storage

- All storage systems should be secure and provide a way for the practice to easily retrieve records if necessary.
- Any external storage sites (both electronic and physical) should be vetted for policies and procedures that apply specifically to medical records.
- Off-site storage may be especially useful for medical practices that are closing and those transitioning from paper to EHR systems.
- Under HIPAA, EHR must be protected by administrative, physical, and technical safeguards so ensure that all storage systems are compliant.

bmdllc.com AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

28

BMD
Brennan Manna Diamond
LISTEN. SOLVE. EMPOWER.

Practical Storage Tip

- Once the retention schedule is complete, you can determine the amount of storage space you have and divide into "Active" and "Inactive" files. Your definition of "active" or "inactive" will depend on the types of files you have, availability of off-site storage, and number of routine patients. As an example:
  - Active files are those for patients who are still being treated or who have been treated in the past year. These files are located in the clinic and are easily accessible to staff.
  - Inactive files can be moved to offsite storage or scanned into an unalterable CD or microfiche. These files will be retained for reference or to meet the retention requirement but you don't anticipate needing access to them routinely.
- If you are using a cloud based system or EHR you will have the ability to have a lot more "active" files that are easily searchable. However, you may need to archive some "inactive" files in order to create more storage space or for cost purposes.
- Set aside time every so often (weekly, monthly, quarterly, etc.) to organize your files and move appropriate folders from "active" to "inactive" status.

bmdllc.com

AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

29

BMD
Brennan Manna Diamond
LISTEN. SOLVE. EMPOWER.

Destruction

- Due to storage constraints, most providers will not be able to retain records indefinitely, so records must be destroyed when legally appropriate.
- As with record retention, there is no single standard destruction requirement.
- Some states require that organizations create an abstract of the destroyed patient information, notify patients when destroying patient information, or specify the method of destruction used to render the information unreadable.
- Organizations should reassess the method of destruction annually based on current technology, accepted practices, and availability of timely and cost-effective destruction services.

bmdllc.com

AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

30

BMD
Brennan Manna Diamond
LISTEN. SOLVE. EMPOWER.

Destruction

- Destruction must be done in a way that makes it impossible to reconstruct the information.
- Examples of destruction methods:
  - For paper records – burning, shredding, pulping, pulverizing.
  - For microfilm or microfiche – recycling and pulverizing.
  - Laser discs used in "write once-read many" document-imaging applications are destroyed by pulverizing.
  - For computerized data – magnetic degaussing or overwriting.
  - DVDs – shredding or cutting.
  - Magnetic tapes – demagnetizing.

bmdllc.com AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

31

BMD
Brennan Manna Diamond
LISTEN. SOLVE. EMPOWER.

Destruction Documentation

- Organizations must permanently maintain documentation of the destruction of health records (usually in a log) and include the following:
  - Date of destruction
  - Method of destruction
  - Description of the disposed records
  - Inclusive dates
  - A statement that the records were destroyed in the normal course of business
  - The signatures of the individuals supervising and witnessing the destruction
- Include any other information relevant to your organization

bmdllc.com AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

32

BMD
Brennan Manna Diamond
LISTEN. SOLVE. EMPOWER.

Destruction Log Example

Destructions Log

Agency					
Division		Section		Branch	
Location(s) of Records					

Records Series	Required Retention	Date Range	Volume (file drawers or MB)	Media (Paper, Electronic)		Date of Destruction	Method of Destruction	Authorization for Destruction
				P	E			

bmdllc.com AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

33

BMD
Brennan Manna Diamond
LISTEN. SOLVE. EMPOWER.

Destruction Plan and Policy

- Tip: Create a record destruction policy and plan, and make sure it is followed.
- Your plan should include your record retention schedule as well as the methods for record destruction.
  - Include built in reminders (monthly, quarterly, etc.) to check to the process to ensure records are retained and destroyed only when appropriate.
  - Include this in your policy: Records involved in any open investigation, audit or litigation should not be destroyed. You should ensure you have a “litigation hold” program in place to preserve all the necessary documentation and evidence in the event of litigation being filed.
  - Develop the workflow for record destruction to ensure each employee knows their role. Only certain individuals should be permitted to destroy medical records so proper destruction methods are followed.
  - Conduct training on medical record retention and destruction with your staff during HIPAA training.

bmdllc.com AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

34

Outsourcing Destruction Services

- Under the HIPAA privacy rule (45 CFR, Parts 160 and 164), when destruction services are outsourced to a business associate (BA), the contract must provide that the BA will establish the permitted and required uses and disclosures and include the following elements:
  - The method of destruction;
  - The elapsed time between acquisition of the records and destruction or disposal;
  - Safeguards against breaches and protocols for notifying the covered entity;
  - Indemnification for the covered entity or provisions for loss due to unauthorized disclosure;
  - Require the BA to provide proof of destruction; and
  - Require the BA to maintain liability insurance at all times.

bmdllc.com AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

35

Notifying Patients of Destruction

- Some states require the notification of patients before you destroy or transfer their medical records.
  - This can be a form letter and should contain no PHI. However, you should identify the types of documents that may be destroyed (e.g. medical record, billing statements, physician/patient conversations).
- Best Practice: Send this letter at least 30 days in advance so patients have enough time to contact you if they would prefer to have their records transferred prior to destruction.
- Keep a record (as part of your log preferably) of when you notified patients and if you received a response from them.

bmdllc.com AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

36

Inadvertent Destruction of Records

- Healthcare providers, including hospitals, physician practices, nursing homes, home health providers, etc. all have legal obligations to maintain and preserve medical records. This is critical in defense of future medical malpractice claims. Improper record keeping has significant consequences. The improper release of medical records and the improper destruction of records can lead to civil and/or criminal liability.
- But what happens if your records are destroyed through a natural disaster or through no fault of your own?
- Typically, if you had no ill intent and the records were destroyed through an "act of God" then you will not be subject to criminal or civil liability.
- If records are lost or damaged, you should conduct and document a risk assessment and develop an action plan.
  - Can any of the records be recreated?
  - Can any records be recovered from digital archived storage?
  - Do patients need to be notified? (This will merge with a HIPAA breach assessment)

bmdllc.com

AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

37

Improper Destruction of Records

- If records are lost or destroyed through a clinician's negligence or intentionally, the practice may be subject to a spoliation claim if a patient or plaintiff in a trial requests that record.
- The improper destruction of evidence, including medical records, which make it so a plaintiff is unable to bring his or her case, can result in the hospital being civilly liable to the patient. This can result even though the records, if kept, may have cleared the hospital and practitioner of negligence in an underlying medical malpractice claim.
  - Example: X-rays inadvertently destroyed when cleaning service thought they were to be thrown out.
- Additionally, CMS's Comprehensive Error Rate Testing (CERT) program that measures improper payments to providers will issue a "no documentation" error if a medical record is missing through the negligence of the provider and cannot be produced.
  - This error will not be produced if the record was destroyed in a natural or man-made disaster like a flood or a fire.

bmdllc.com

AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

38

BMD
Brennan Manna Diamond
LISTEN. SOLVE. EMPOWER.

Ancillary Records

- In addition to the medical record, there are ancillary materials that could contain PHI and need to be destroyed in a timely manner:
  - Carbon copies, duplicates, or misprints
  - Advanced directives
  - E-mails (patient to provider, provider to provider)
  - Faxes
  - Videos of patient
  - Waiting room records
  - Cell phones! Any electronic device that does not have a hard drive must be reset to factory defaults prior to reuse.
- If these are not part of the medical record, they do not need to be maintained for a specific period of time.
  - However, they should be allocated to a specific retention period if possible and destroyed when that period passes as with any other form of confidential information.

bmdllc.com AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

39

BMD
Brennan Manna Diamond
LISTEN. SOLVE. EMPOWER.

Destruction of Non-Medical Records

- Many other business records have their own retention schedules and may only be destroyed after a certain amount of time. Examples:
  - OSHA: Employee Medical Records must be kept for the duration of employment plus 30 years. Exposure records must be kept for 30 years. The OSHA 300 Log of all recordable occupational injuries and illnesses must be kept for 5 years following the end of the year to which they relate.
  - Tax Documents: IRS requires you to keep records for 3 years from the date you filed your original return or 2 years from the date you paid the tax, whichever is later (plus additional time if you file a claim for a loss).
    - Tax returns, auditors' reports and annual financial statements should be kept indefinitely.
  - Credit card records: At least 18 months to ensure you can fight any chargebacks that may occur. Longer if needed for tax purposes.

bmdllc.com AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

40

BMD
Brennan Manna Diamond
LISTEN. SOLVE. EMPOWER.

Examples

bmdllc.com

AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

41

BMD
Brennan Manna Diamond
LISTEN. SOLVE. EMPOWER.

Example #1

- What if my patient dies? Can I be done with retention laws then?
  - No! HIPAA does not end if a client dies.
  - Record retention requirements still apply, even after death.
  - Record disclosure laws also apply, information cannot be shared beyond the deceased patient's personal representative without consent.

bmdllc.com

AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

42

LISTEN. SOLVE. EMPOWER.

Real Life Example #1: CVS

- January 16, 2009, the U.S. Department of Health & Human Services (HHS) reached agreement with CVS Pharmacy, Inc. to settle potential violations of the HIPAA Privacy Rule.
- Among other issues, the OCR review indicated that:
  - CVS failed to implement adequate policies and procedures to reasonably and appropriately safeguard protected health information during the disposal process;
  - CVS failed to adequately train employees on how to dispose of such information properly; and
  - CVS did not maintain and implement a sanctions policy for members of its workforce who failed to comply with its disposal policies and procedures.
- Under the Resolution Agreement, CVS agreed to pay a $2,250,000 resolution amount and implement a strong Corrective Action Plan that requires:
  - revising and distributing its policies and procedures regarding disposal of protected health information;
  - sanctioning workers who do not follow them;
  - training workforce members on these new requirements;
  - conducting internal monitoring;
  - engaging a qualified, independent third-party assessor to conduct assessments of CVS compliance with the requirements of the Corrective Action Plan and render reports to HHS;
  - new internal reporting procedures requiring workers to report all violations of these new privacy policies and procedures; and
  - submitting compliance reports to HHS for a period of three years.

bmdllc.com

AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

43

LISTEN. SOLVE. EMPOWER.

Real Life Example #2: Filefax

- In Feb. 2018, HHS announced a $100,000 settlement with Filefax, a company that provided medical record storage and disposal. Based on an anonymous complaint, HHS found that Filefax impermissibly disclosed PHI by:
  - leaving PHI in an unlocked truck in the Filefax parking lot, and
  - granting permission to an unauthorized person to remove the PHI from Filefax and leaving the PHI unsecured outside the Filefax facility.
- OCR confirmed that an unauthorized individual retrieved these medical records and attempted to sell them at a shredding and recycling facility.
- This is an important case because Filefax is a BA and Filefax closed its doors a year before the HHS settlement. Therefore, BAs can be held responsible for breaches and going out of business does not necessarily help you avoid liability.

bmdllc.com

AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

44

BMD
Brennan Manna Diamond
LISTEN. SOLVE. EMPOWER.

Questions?

Daphne Kackloudis, Esq.
(614) 246-7508
dlkackloudis@bmdllc.com

Ashley Watson, Esq.
(614) 246-7518
abwatson@bmdllc.com

bmdllc.com AKRON CANTON CLEVELAND COLUMBUS BONITA SPRINGS JACKSONVILLE

45