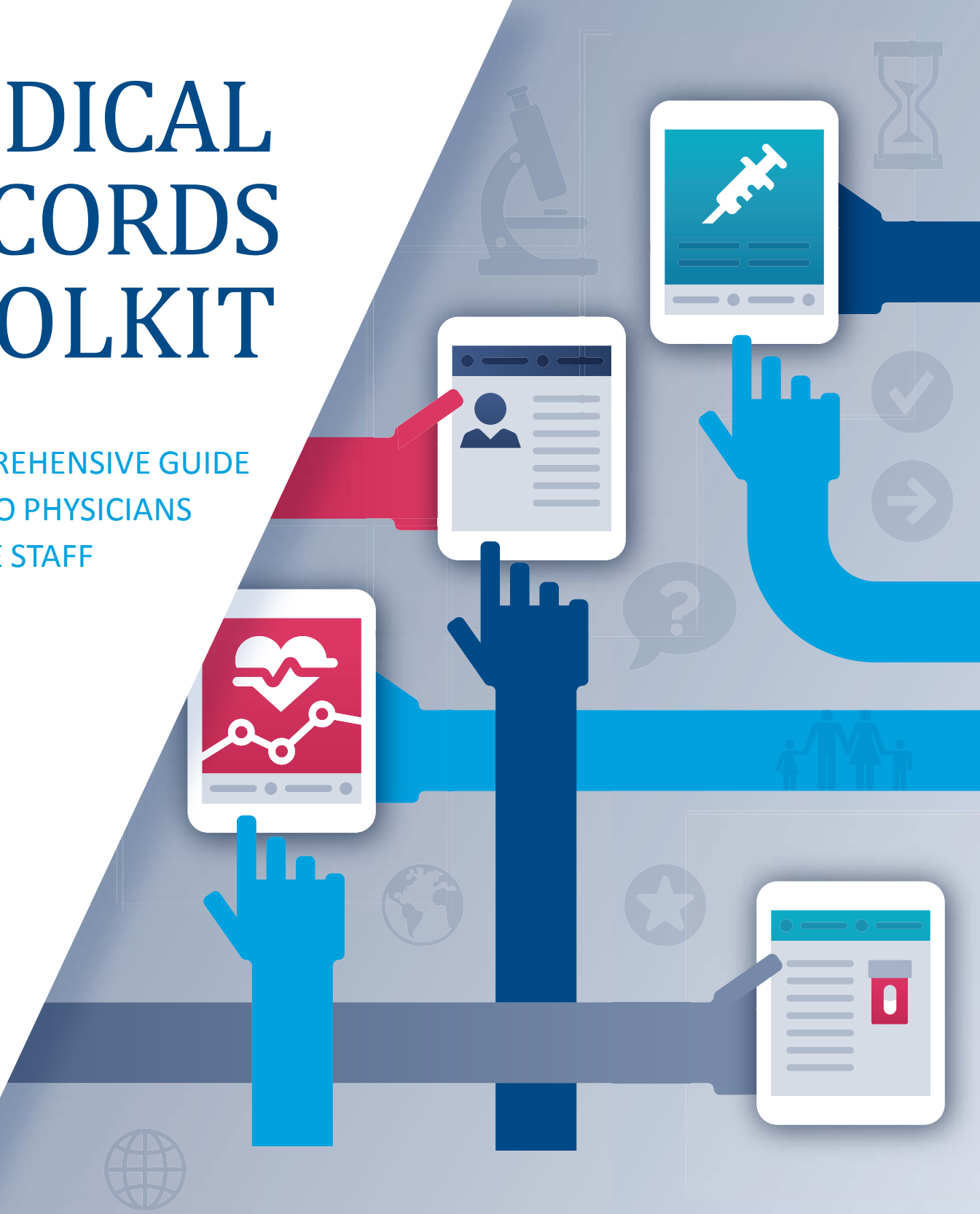
MEDICAL RECORDS TOOLKIT

A COMPREHENSIVE GUIDE FOR OHIO PHYSICIANS & OFFICE STAFF



Ohio State Medical Association

VER. 5.2020

Bringing physicians together for a healthier Ohio

CONTENTS

COVID-19 ADDENDUM (MAY 2020)

SECTION 1: Medical Record Components

SECTION 2: Discharging a Patient

SECTION 3: Release of Records

SECTION 4: Notice of Privacy Practices

SECTION 5: HIPAA Compliance & Applicable Ohio Law

SECTION 6: Amendment of Records

SECTION 7: Retention, Storage, Transfer, Safeguards & Destruction

INTRODUCTION

Medical records are one of the most important parts of a medical practice. They provide documentation for treatment, allow for continuity of care and can serve as evidence in a legal setting. With the number of functions medical records can serve, making sense of the various laws which govern them can be a confusing and daunting task. This guide aims to alleviate the regulatory, legal and ethical concerns associated with the managing medical records in a medical practice.

As you read this guide, you will find important statutory information cited within the body of the text. Please refer to the Tools and Resources section for information on where to find the regulations cited.

This guide was developed for general informational purposes only. It should not be construed as authoritative legal advice. The information contained in this guide was developed in March 2014 and reviewed/updated May 2020. However, users should review the most current version of the cited code sections and other cited references.

MEDICAL RECORDS TOOLKIT

A COMPREHENSIVE GUIDE
FOR OHIO PHYSICIANS
& OFFICE STAFF

COVID-19
ADDENDUM
(MAY 2020)

HIPAA DURING COVID-19

WHAT'S CHANGED?

During the COVID-19 public health emergency, the HHS Office for Civil Rights (OCR) issued guidance about how the HIPAA Privacy and Security Rules allow patient information to be shared in an outbreak of infectious disease as well as to assist patients in receiving the care they need. To the extent that HHS announced any easing of HIPAA requirements, these rule modifications or easing of enforcement of the rules are temporary and only in effect for the duration of the COVID-19 public health emergency.

SUMMARY OF HIPAA MODIFICATIONS ANNOUNCED BY HHS:

1. Guidance on how health care providers can share information with the Center for Disease Control (CDC) or state and local health departments, family members of patients, and others, to help address the COVID-19 emergency. Much of what is addressed is allowed by HIPAA under normal operations such as disclosures for treatment, disclosures to family, friends and others involved in a patient's care and disclosures for public health activities.

2. Disclosures of Protected Health Information about Individuals Exposed to COVID-19 to First Responders and Others – this type of disclosure is permitted, without HIPAA authorization, when for example, needed to provide treatment, when required by law, when disclosure is necessary to prevent or lessen a serious and imminent threat. Health care providers must, however, make reasonable efforts to limit the disclosure of PHI to that which is "minimum necessary" to accomplish the purpose of the disclosure.

3. Telehealth Remote Communications – HHS is exercising enforcement discretion to not impose penalties for HIPAA violations in situations where use of telecommunications technology would normally violate HIPAA privacy, security, or breach notification rules. The goal is to allow health care providers to use telehealth to treat patients remotely when possible during this public health emergency. Note that this enforcement discretion applies only to telehealth and does not affect how HIPAA applies outside of telehealth during this time. HHS has issued Guidance FAQs that explain how the enforcement discretion works: ***www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html***

   See also the OSMA's telehealth webpage for comprehensive information about how to implement telehealth for your practice: ***www.osma.org/telehealth-faq***

   The Substance Abuse and Mental Health Services Administration (SAMSHA) has issued similar guidance with respect to the confidentiality of substance abuse patient records.

   Even if enforcement is eased during the COVID-19 epidemic, consider implementing these best practices mentioned by the Office for Civil Rights when using telehealth tools:

   - Notify patients that use of the application may introduce some privacy risks.
   - Enable all encryption capabilities and privacy modes.

- Use vendors that provide a nonpublic-facing product, so only the intended parties are allowed to participate in the communication.
- Use a HIPAA-compliant vendor and enter into a business associate agreement with the vendor. This positions you to continue to use the platform for telehealth services when appropriate if you choose after the COVID-19 emergency is lifted.

4. Participating in Community Based Testing Sites – this announcement gives health providers guidance about how to participate in and treat patient privacy at community based testing sites.

WHAT HIPAA RULES HAVE NOT CHANGED?

Unless specifically addressed in an HHS announcement that applies during the COVID-19 public emergency period, all HIPAA rules remain in full force and effect for routine patient care. So, for example, medical practices should continue to follow all of your HIPAA compliant policies and procedures addressing, but not limited to, notices of privacy practices, requests for medical records, limiting disclosures to the minimum necessary to accomplish the purpose of the disclosure, limiting incidental disclosures and authorizations to release information. Physician practices should also ensure that they are following security rule provisions to protect privacy.

Notably, civil rights laws also continue in effect during the state of the public health emergency meaning that health care practices should not discriminate against patients with disabilities or who are otherwise protected against discrimination on the basis of race, color, national origin, disability, age, sex, and exercise of conscience and religion. Persons with disabilities should not be denied medical care on the basis of stereotypes, assessments of quality of life, or judgments about a person's relative "worth" based on the presence or absence of disabilities or age. Decisions about whether an individual is a candidate for treatment should be based on an individualized assessment of the patient and his or her circumstances, based on the best available objective medical evidence.

All HHS announcements regarding HIPAA during COVID-19 are available at https://www.hhs.gov/hipaa/for-professionals/special-topics/hipaa-covid19/index.html Please read the full announcements for a complete understanding of HIPAA compliance during the COVID-19 public health emergency.

Separate, but related, CMS also announced easing of compliance requirements related to the Interoperability and Patient Access final rules adopted as part of the 21st Century Cures Act. These rules address information sharing of and patient access to electronic health information. See https://www.cms.gov/Regulations-and-Guidance/Guidance/Interoperability/index

WEBINAR RECORDING: *OCR UPDATE ON HIPAA & COVID-19* (4/29/2020)

The HHS Office for Civil Rights (OCR) hosted a webinar on April 24, 2020, for health IT stakeholders on HIPAA privacy and security issues related to COVID-19 and recent OCR actions related to the pandemic.

To access the recording, visit:
https://youtu.be/2C6iOdS_FR0

The slides from this presentation are also available:
https://go.usa.gov/xvExS

TOPICS INCLUDE:

1. COVID-19 and Permissible Disclosures under the HIPAA Privacy Rule
2. Enforcement Discretion and Guidance for Telehealth Remote Communications
3. Guidance for Disclosures to First Responders and Public Health Authorities
4. Enforcement Discretion for Business Associates to Use and Disclose PHI for Public Health and Health

OVERSIGHT ACTIVITIES:

1. Enforcement Discretion for Community-Based Testing Sites

COVID-19
ADDENDUM
(MAY 2020)

MEDICAL RECORD DOCUMENTATION DURING COVID-19

During the COVID-19 epidemic, physicians should continue their normal medical documentation practices where possible. It is likely, however, that during the epidemic many physicians are using telehealth for diagnosis and treatment and the nature of the platform/visit precludes some services that would normally take place.

For telehealth visits, or where an in-person visit is not possible, it may be that the physician cannot provide the same course of treatment for a variety of reasons such as scare resources or due to government directives to avoid nonessential medical procedures. To the extent that a physician continues to see patients during COVID-19, what sort of documentation might be helpful? There are no clear answers, but what follows are some suggestions for your consideration.

It may be helpful to make a simple notation in the chart like "NOTE: This encounter occurred during the COVID-19 pandemic crisis." This notation puts persons reading a chart, after the fact, of the circumstances that led to the treatment decisions documented in the chart at the time of treatment. Physicians are held to the standard of what physicians in the same or similar circumstances would do. Some type of reference to the COVID-19 epidemic puts persons on notice of the conditions that were in place during the visit that may have led to treatment decisions, actions, or inactions.

Consider if any specific documentation is warranted because the treatment rendered is in support of COVID-19 response. And conversely, is any documentation warranted because of limitations on treatment, outside of direct COVID-19 support, due to government orders or other limitations resulting from the epidemic? Generally, more documentation is better than less. As always, physicians should consult their professional liability carriers for recommendations about documentation during a time when the standard of care is disrupted by an epidemic or other emergency or disaster.

END

COVID-19
ADDENDUM

(MAY 2020)

SECTION 1

MEDICAL RECORD COMPONENTS

FORMAT

Consistency and ease of use should be the number one priority in creating a medical records system. Regardless of the format chosen, every physician and staff member should be able to access a record and easily understand the patient's current condition, past medical history and all other entries. Importantly, key identifiers for a patient should be recorded consistently and be visible on each page of a patient's records.

BEST PRACTICE TIP

In a paper records system, consider placing the patient's name, date of birth and/or patient identifier number at either the top of the record or with side tabs on EVERY page of a paper file. If both sides of a page have information, mark the patient's name clearly on the second side.

USE OF TEMPLATES

The use of a template will create the consistency and ease a medical practice needs to run efficiently. A template will ensure the same information is recorded for each patient and no information is inadvertently missed. Templates also facilitate dictation and transcription. However, like all methods of standardization, templates can lead physicians to rush through a dictation, causing repetition in entries to the point of inaccuracy.

Electronic Health Records (EHRs) have the benefit of a built-in template system, with default settings, dropdown boxes and checklists. Another convenient feature is the ability to copy and paste information from one entry to the next. However, physicians and staff should use caution when copying and pasting information from one entry to the next to ensure the copied notes actually pertain to the date of service to which they were added. Templates with check boxes, predefined answers or dropdown menus may also fail to meet certain coding requirements if they do not provide sufficient space for documentation

LEGIBILITY

When creating or revamping a medical records system, the importance of a legible record cannot be overstated. For all "health care facilities" in Ohio, the legibility of medical records is a requirement.[1] Illegible records can create injury for patients, particularly in the way of medication errors. They can also create inefficiency within a practice. Not only is a legible record important for the safety of patients, it is also important for liability reasons. For example, medical records may be a key piece of evidence in a medical liability suit. The legibility of the record in question may determine liability. In Medicare Recovery Audit Contractor (RAC) audits or other various investigations, medical records can be discounted for illegibility.

BEST PRACTICE TIP

Create a practice-wide policy for the format of patient medical records, including the use of templates. Make sure all physicians and staff are thoroughly trained on what office policy entails, how to use the templates and what is to be included in every record.

1. *Ohio Administrative Code Section 3701-83-11. "Health care facilities" include ambulatory surgical centers, freestanding dialysis center, freestanding birthing center, freestanding inpatient rehabilitation center, freestanding radiation therapy center and freestanding or mobile diagnostic imaging center.*

TYPICAL CONTENT

While the content of medical records will be dictated by the medical specialty and the reason for the patient's visit, at a minimum the following information should be included.

DOCUMENTATION IN A RECORD

Documentation in a medical record can be tricky. If certain information is left undocumented, it could have serious ramifications for a practice. Here are some common concerns.

1. **PATIENT NONCOMPLIANCE:** patient noncompliance should always be documented in a patient's record. Noncompliance should be noted clearly and factually. Even suspicion of noncompliance should be noted. Also document patient education efforts and attempts to bring the patient into compliance.

1. **LEGAL ISSUES:** a litigious patient should not be treated differently from any other patient. Visits should be charted like normal.

2. **FINANCIAL DISPUTES:** billing and collections activities should not be part of the patient's medical records. This should be recorded in the patient's financial records.

3. **DRUG-SEEKING BEHAVIOR:** a patient's drug seeking behavior should be accurately and factually recorded, and may include a copy of OARRS (Ohio Automated RX Reporting System) reports that you run on the patient. See ***www.ohiopmp.gov***

4. **CONSULTATIONS:** the nature and scope of a formal consultation should be clearly indicated in a record. Avoid over-documenting informal conversations or inquiries.

5. **PATIENT'S CONCERNS ABOUT ANOTHER PHYSICIAN:** these concerns do not belong in a patient's medical record. If records received from another physician or provider conflict with information reported by the patient, the current physician should note the inconsistency.

6. **PHYSICIAN'S CONCERNS ABOUT PRIOR MEDICAL CARE:** while legitimate concerns about another physician's quality of care should be reported as appropriate or required, a patient's medical record is not the appropriate avenue to report those concerns.

BEST PRACTICE TIP

At a minimum, the checklist below should ALWAYS be included in a patient's medical records. But to ensure records are as accurate and as complete as possible, be mindful of the following.

- Notate any medication allergies in a readily, observable manner. For records kept in hardcopy, a bright sticker is recommended. EHR's should have an automatic alert function for any allergy
- Avoid all forbidden abbreviations
- Include records received from other physicians or health care professionals
- Include properly identified photographs, images or videos
- Include information containing significant clinical content received via telephone, email or text messaging
- Proofread before signing
- Document any patient noncompliance to treatment or advice
- Document the disclosure of informed consent

MEDICAL RECORD CHECKLIST:

- ❑ *Date of Service*
- ❑ *Name and Patient Identifiers*
- ❑ *Vitals and Medications*
- ❑ *Patient Complaints/Problem*
- ❑ *History of Problem*
- ❑ *Review of Systems*
- ❑ *Past Histories*
- ❑ *Results of Exams, Labs, Tests*
- ❑ *Treatment Instructions*
- ❑ *Other Recommendations and Educational Material*
- ❑ *Signature of Professional*

TEXT MESSAGES & EMAILS FROM PATIENTS

Emailing and text messaging to communicate health information is permitted under HIPAA. Emailing and texting messaging to and from patients is becoming increasingly common, and precautionary measures must be taken so no breach occurs. The use of email and text messaging can increase a practice's efficiency and lower costs. The use of email is ideal for things such as prescription refill requests and to schedule appointments. Of course, a practice can always refuse to use either method of communication with patients.

EMAIL:

If a practice decides to use email communications with patients, an encrypted email is recommended although not required under HIPAA. A patient may request personal health information (PHI) be sent via unencrypted email. The patient must be advised of the risk this involves and still request this form of transmission before any PHI can be sent via unencrypted email to the patient (45 CFR 164.524(c)(2)(ii)).

Information sent by a patient in an email should be treated just like any other information obtained by a practice from a patient. The information should be documented in the patient's record. If the practice retains hard copy records, the email should be printed and filed accordingly. Practices using electronic records should save the email in the patient's e-file.

TEXT MESSAGING:

Text messaging can be used to communicate health information, both to patients and among providers. The main concern with sending text messages containing PHI is that the messages are generally not secure and the sender does not know with certainty if a message is received by the intended recipient. Furthermore, wireless carriers may store the text messages.

However, a practice may perform a risk analysis and determine text messaging to be low risk or implement a third party messaging solution that incorporates security measures to allow text messaging from approved mobile devices. If a practice does decide to utilize text messaging as a form of communication with patients, the communication should be documented in the patient's record. Here are some safeguards a practice can use to help protect and secure information sent via text message:

1. Use a password or other user authentication.
2. Install and enable encryption.
3. Install and activate remote wiping and/or remote disabling.
4. Disable and do not install or use file sharing applications.
5. Install and enable a firewall.
6. Install and enable security software.
7. Keep your security software up-to-date.
8. Research mobile apps before downloading.
9. Maintain physical control of the device.
10. Use adequate security to send or receive health information over public Wi-Fi networks.
11. Delete all stored health information before discarding or reusing the device.

BEST PRACTICE TIP

If your practice wishes to communicate with patients via email, the patient should sign a statement to be kept in his or her record acknowledging his or her desire for email communication and understanding of the risks involved. The statement should also include what types of communications are not appropriate for email communication such as emergencies and sensitive information like mental health or HIV status.

BEST PRACTICE TIP

Be careful when text messaging with your patients. Consider using text messages as alerts to have your patients contact the practice by telephone. If your practice wishes to text with patients, follow the safeguard tips for making the communication as secure as possible.

ORGANIZATION OF PAPER RECORDS

While electronic records are now the norm, many practices continue to use hard copy medical records. Organization in a system of paper records is paramount to a practice's success, yet can be difficult to achieve.

FILING OF RECORDS:

The development of a user-friendly and organized filing system for patient records is extremely important for a practice that continues to use hard copy medical records. Records can be filed alphabetically, by date of birth and alphabetically, by the last four digits of a social security number, or with a unique patient number.

Electronic records now eliminate many of the organizational issues associated with hard copy records. It is less likely a record will be "misplaced," and records can be archived and backed up on another system to eliminate the possibility of a lost record.

STRAY RECORDS:

Every paper record should either be properly filed when not in use or in use for a particular purpose such as a patient visit, telephone call, dictation, compliance review, etc. Practices should develop a system of notification for records in use. For example, when a record is removed from filing, an "out card" identifying the location of the record and the name of who removed the record should be left in the record's place.

RECORDS LEAVING THE OFFICE:

Original records should rarely leave the office. A significant number of HIPAA violations/data breaches (and possible fines) occur when a device containing medical records is taken out of the office and then is stolen or misplaced. On occasion, a record may need to be moved to a different office location within a practice or to legal counsel. In the event a record must be moved, make a copy first. Create an office policy for use of records outside the office and adhere to it. Maintain a meticulous list (perhaps in a spreadsheet) of the records out of the office.

BEST PRACTICE TIP

Label medical records using more than one key identifier. For example, using only a patient's name could result in a case of mistaken identity if the practice has more than one patient with the same name.

MODIFICATIONS AND CORRECTIONS

Generally, the two ways to modify a patient's medical record is through a late entry or the documentation of an error.

A late entry is any notation added to a previously signed and dated record. To properly add a late entry, the provider should accurately document the misstated or missing information and label it as a "late entry." Indicate the date and time when the additional note is added.

Mistakes sometimes occur. Proofreading or systems of dictation/transcription can alleviate the majority of errors. Should a correction to a record need to be made, draw a line through the incorrect entry, write "error" above the lined-out entry and date and initial the entry.

NOTE:
ELECTRONIC SIGNATURES

Technological advances regarding EHRs may lead to concerns about the authenticity of a provider's electronic signature. Although HIPAA does not have an electronic signature standard, an EHR system can limit input access strictly to the signer by using authenticated electronic signatures.

SECTION 2

DISCHARGING A PATIENT

TERMINATION OF THE PHYSICIAN-PATIENT RELATIONSHIP

Once a physician-patient relationship is established, the relationship continues until the relationship is terminated. Ohio law requires a physician who terminates his or her relationship with a patient to notify the patient. Here are the required notification steps (OAC Section 4731-27-02).

NOTICE MUST BE SENT TO THE PATIENT AND IS TO INCLUDE THE FOLLOWING:

1. A statement that the physician-patient relationship is terminated.
2. A statement that the physician will continue to provide emergency treatment and access to services for up to 30 days from the date of the letter.
3. An offer to transfer the patient's records to a new provider upon the patient's authorization to do so.

NOTICE MUST BE SENT ONE OF THE FOLLOWING WAYS:

1. Certified mail, return receipt requested, to the patient's last address on record. Retain a copy of the letter, the certified mail receipt and the mail delivery receipt in the patient's records.
2. Electronic message via a HIPAA compliant electronic medical record system or EHR system. The system must be capable of sending notification to the patient that the message has been received and is capable of notifying the sender whether a message has or has not been viewed.

OF COURSE, THERE ARE EXCEPTIONS TO THIS RULE. THE ABOVE REQUIREMENTS DO NOT APPLY WHEN:

1. A physician rendered medical services to a patient on an episodic or emergency basis and the physician does not reasonably expect to render future medical services to the patient.
2. A physician formally transferred the patient's care to another provider not in the physician's practice group.
3. A physician is leaving a practice, selling a practice, retiring, or whose employment with a healthcare entity has ended.
4. The patient either verbally or in writing terminated the relationship or transferred care to another physician for the same or related condition. The physician should document in the patient's records that the patient has terminated the relationship.

BEST PRACTICE TIP

While Ohio law requires physicians to give at least 30 days notice to patients they have treated in the last two years, it is preferable to give notice two to three months prior to the closing date. Also, if there is any uncertainty as to whether a patient was treated within the last two years, the patient should be treated as an active patient for purposes of notification.

PHYSICIAN IS FIRED, LEAVES A PRACTICE, SELLS A PRACTICE OR RETIRES

In the event a physician's employment is terminated or he/she leaves a practice, sells a practice or retires, his/her patients must be notified (OAC Section 4731-27-03). Notice can be given by the health care entity or the entity may give the physician a list of patients with contact information. At least 30 days notice must be given to patients that a physician treated in the last two years. The notice must advise patients of the opportunity to transfer records or provide contact information to obtain any records remaining in the physician's possession after he or she no longer sees patients.

NOTICE MUST BE GIVEN IN ONE OF THE FOLLOWING WAYS:

1. Via regular mail to patients seen by the physician within the last 2 years. Physicians (or the entity providing notice) must also document the date the letter was mailed.
2. An electronic message sent via a HIPAA compliant EMR/EHR system that provides a means of electronic communication between the health care entity and patient and is capable of sending the patient a notification that a message has been received and is in the patient's portal.
3. The physician may, but is not required to publish notice in the newspaper.

BEST PRACTICE TIP

If the physician is not able to provide the 30-day notice due to acute illness or an unforeseen emergency, the notice must be given no later than 30 days after it is determined that the physician will not be returning to the health care entity.

WHEN LEAVING, SELLING, OR RETIRING FROM AN ENTITY WHERE A PHYSICIAN HAS PROVIDED PHYSICIAN SERVICES AS AN OWNER OR INDEPENDENT CONTRACTOR

THE NOTICE SHALL INCLUDE THE FOLLOWING:

1. A statement that the physician will no longer be practicing medicine at the health care entity;
2. The date on which the physician ceased or will cease to provide medicine services at the health care entity;
3. If the physician will be practicing medicine in another location, contact information for the physician subsequent to leaving the health care entity;
4. Contact information for an alternative physician or physicians employed by the health care entity, or contact information for a group practice that can provide care for the patient; and,
5. Contact information that enables the patient to obtain information on the patient's medical records.

FOR MORE INFORMATION ON CLOSING A PRACTICE

See the American Academy of Family Physicians (AAFP) checklist at:

www.aafp.org/dam/AAFP/documents/practice_management/admin_staffing/ClosingPractice-Checklist.pdf

SECTION 3

RELEASE OF RECORDS

RESPONDING TO REQUESTS

THERE ARE GENERALLY TWO TYPES OF REQUESTS FOR RECORDS:

1. Requests from other providers for routine information to facilitate care.
2. Formal records requests.

For routine information moving from provider to provider, records may be sent to another provider or accessed via an EHR system for treatment purposes. Formal records requests come from patients, the families of patients or attorneys for a variety of reasons. Ohio law permits a patient, a patient's personal representative or an authorized person to submit a request to examine or obtain a copy of a medical record (ORC Section 3701.74(B)).

IN ORDER FOR THE REQUEST TO BE VALID, IT MUST:

1. Be in writing.
2. Be signed by the patient, personal representative or authorized person.
3. Dated not more than one (1) year before the date on which it is submitted.
4. Indicate where the copy of the records is to be sent.

According to guidelines issued by the U.S. Department of Health and Human Services, providers cannot require that a patient give a reason for requesting copies of their medical records. Doctors and hospitals also cannot require patients to retrieve their records in person if they have asked that the records be sent to them via mail or email.

A patient's request cannot be denied due to the patient's failure to pay medical bills. Providers also may not deny the requested PHI merely out of concern that the patient might be upset by it. However, under the new rules, providers may refuse to disclose the information if it is "likely to endanger the life or physical safety" of the patient or of another individual.

A provider must provide an individual with access to PHI in the form and format requested by the individual, if it is readily producible as such. If it is not readily producible, it must be provided in a readable hard copy form or other form and format as agreed to by the provider and the individual. A health care provider that utilizes electronic records must provide electronic information to an individual in the electronic form and format requested by the individual, if it is readily producible. If it is not readily producible, it must be produced in a readable electronic form and format as agreed to by the provider and the individual (45 CFR Section 164.524(c)).

REMEMBER:

Providers cannot require that a patient give a reason for requesting copies of their medical records. Doctors and hospitals also cannot require patients to retrieve their records in person if they have asked that the records be sent to them via mail or email.

HIPAA PROVIDES SOME EXCEPTIONS TO THE RIGHT OF PATIENTS TO OBTAIN COPIES OF THEIR MEDICAL RECORDS INCLUDING:

1. Psychotherapy notes.
2. Notes made in preparation for legal matters.
3. Research records: An individual's access to health information maintained by a researcher or covered health care provider in a clinical trial may temporarily be rescinded. HIPAA allows the provider or researcher to suspend the access rights of the individual while the clinical trial is still in progress, as long as the research participant has agreed to this denial of access when consenting to participation in the clinical trial itself. The provider or researcher must also tell the participant that their rights to access the protected health information will be restored at the conclusion of the clinical trial.
4. Information from a third party who is not a physician or provider bound by a promise of confidentiality.
5. Exceptions with a "right of review" (45 CFR Section 164.526(a)(1)).

INSTANCES WHERE MEDICAL RECORDS MAY BE RELEASED

1. **MENTAL HEALTH RECORDS:** a patient must be granted access to the patient's own psychiatric and medical records, unless access is specifically restricted in a patient's treatment plan for clear treatment reasons (ORC Section 5122.31). The disclosure of mental health information, like all PHI, must comply with all HIPAA regulations. Psychotherapy notes as defined by HIPAA rules are excepted. Below is clarification regarding HIPAA rules applicable to mental health records.
    - Under 45 CFR. Section 164.510(b), health care providers may communicate with a patient's family members and friends when the patient does not object and the disclosures are directly relevant to that person's involvement in the patient's care or payment for care.
    - A provider is permitted to disclose mental health information to friends or family when a patient is not present or is unable to agree or object due to incapacity or emergency circumstances and the provider believes it is in the patient's best interests (45 CFR Section 164.510(b)(3)).
2. **MINOR MENTAL HEALTH RECORDS:** a provider may disclose PHI to a parent or guardian as the personal representative of a minor child (45 CFR Section 164.502(g)) with some exceptions.
    - A parent is not treated as a minor's personal representative when Ohio law or other law does not require the consent of a parent before a minor can obtain a particular health care service, the minor consents to the service, and the minor has not requested the parent be the personal representative.
    - Someone besides the parent is authorized by law to consent to the service and provides such consent.
    - A parent agrees to a confidential relationship between the minor and provider with respect to the service.

FOR MORE INFORMATION:

REFERENCE
CODE OF FEDERAL REGULATIONS
45 CFR Section 164

3. **HIV STATUS:** Although HIPAA does not provide special protection for HIV information, Ohio law does provide special protection (ORC Section 3701.243). HIV test results are confidential, except that they may be released to:
    - The individual tested, the individual's legal guardian, spouse or any sexual partner;
    - A person to whom disclosure is authorized by a written release;
    - The individual's physician;
    - Department of health or health commission if reporting is required;
    - An organ donation facility if medical information is needed about the deceased to render an organ acceptable for donation;
    - Health care facility staff committees or accreditation or oversight review organizations conducting program monitoring, program evaluation, or service reviews;
    - A health care provider, emergency medical services worker, or peace officer who sustained significant exposure to the body fluids of another individual, and the identity of the tested individual must not be revealed;
    - Law enforcement authorities pursuant to a search warrant or a subpoena in connection with a criminal investigation or prosecution; and
    - A health care provider, or an authorized agent or employee of a health care facility or a health care provider, if the provider, agent, or employee has a medical need to know the information and is participating in the diagnosis, care or treatment of the individual on whom the test was performed.
4. **DRUG OR ALCOHOL RECORDS:** Must be kept confidential unless the patient gives consent to release the records in writing (ORC Section 5119.27). Federal law also governs the confidentiality of drug and alcohol abuse records obtained by federally assisted drug or alcohol abuse program (42 CFR Section 2.12).
5. **IN AN EMERGENCY:** a provider must release medical records to expedite the best care possible for the patient and the patient's permission to release the records is not needed (45 CFR Section 164.506).

MEDICAL RECORD COPYING CHARGES

Both HIPAA and Ohio law permit health care providers and medical records companies to charge fees for copies of medical records. HIPAA permits reasonable, cost-based fees for copies of information, plus labor and supply costs, but does not permit charging for search and retrieval costs (45 CFR 164.524). Ohio annually adjusts copying fees that are authorized by statute (See below). Note that HHS does not approve of per page copying charges for electronically maintained records. HHS has opined that *"a covered entity may charge individuals a flat fee for all requests for electronic copies of PHI maintained electronically, provided the fee does not exceed $6.50, inclusive of all labor, supplies, and any applicable postage.*

BEST PRACTICE TIP

Consider posting a copy of fee charges in the office or providing a copy to patients.

Charging a flat fee not to exceed $6.50 is therefore an option for entities that do not want to go through the process of calculating actual or average allowable costs for requests for electronic copies of PHI maintained electronically." See HHS OCR FAQs on access to records.

Physicians should inform patients of fee charges by posting a notice in the office or as part of Notices of Privacy Practices given to patients.

Even though the law permits charging fees for copying records, the federal 21st Century Cures Act (CURES Act) encourages giving patients free and easy access to electronic health records and encourages the free flow of health information among health care providers for treatment purposes. Thus, HHS OCR, in its records access FAQs suggests that "covered entities should provide individuals who request access to their information with copies of their PHI free of charge. While covered entities should forgo fees for all individuals, not charging fees for access is particularly vital in cases where the financial situation of an individual requesting access would make it difficult or impossible for the individual to afford the fee. Providing individuals with access to their health information is a necessary component of delivering and paying for health care. We will continue to monitor whether the fees that are being charged to individuals are creating barriers to this access, will take enforcement action where necessary, and will reassess as necessary the provisions in the Privacy Rule that permit these fees to be charged."

Notably, a federal district court has ruled that HHS overstepped its authority regarding the issue of medical record copying charges as applied to requests by "third parties." Thus HHS FAQs that address access to records, including the FAQs that address copying charges include this statement: This guidance remains in effect only to the extent that it is consistent with the court's order in Ciox Health, LLC v. Azar, No. 18-cv-0040 (D.D.C. January 23, 2020), which may be found at ***https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2018cv0040-51***

More information about the order is available at:
www.hhs.gov/hipaa/court-order-right-of-access/index.html

Any provision within this guidance that has been vacated by the Ciox Health decision is rescinded.

AS A RESULT OF THE CIOX LAWSUIT, HHS HAS POSTED THIS NOTICE:

> ***Important Notice Regarding Individuals' Right of Access to Health Records***
>
> *On January 25, 2013, HHS published a final rule entitled "Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act, and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules." (2013 Omnibus Rule). A portion of that rule was challenged in federal court, specifically provisions within 45 C.F.R. §164.524, that cover an individual's access to protected health information. On January 23, 2020, a federal court vacated the "third-party directive" within the individual right of access "insofar as it expands the HITECH Act's third-party directive beyond requests for a copy of an electronic health record with respect to [protected health information] of*

BEST PRACTICE TIP

Note that Ohio copying charges are adjusted annually—typically in February.

an individual ...in an electronic format." Additionally, the fee limitation set forth at 45 C.F.R. § 164.524(c)(4) will apply only to an individual's request for access to their own records, and does not apply to an individual's request to transmit records to a third party. (emphasis added)

The right of individuals to access their own records and the fee limitations that apply when exercising this right are undisturbed and remain in effect. OCR will continue to enforce the right of access provisions in 45 C.F.R. § 164.524 that are not restricted by the court order. A copy of the court order in Ciox Health, LLC v. Azar, et al., No. 18-cv-0040 (D.D.C. January 23, 2020), may be found at: https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2018cv0040-51

Because of the statutory, regulatory and other legal changes that affect access to records and copying charges, the OSMA strongly encourages physicians to review all of the HHS Office for Civil Rights FAQs on its website for health professionals that address a patient's right to access their protected health information. View these FAQs at:
www.hhs.gov/hipaa/for-professionals/faq/right-to-access-and-research/index.html

Practices might also consult with legal counsel to develop appropriate office policies around medical record copying charges.

NOTE THAT THE FOLLOWING OHIO STATUTORILY AUTHORIZED COPYING FEES ARE ONLY PERMITTED TO THE EXTENT THAT THEY ARE THE SAME TYPES OF COSTS PERMITTED UNDER 45 CFR 164.524(C)(4) OF THE HIPAA PRIVACY RULE, AND ARE REASONABLE.

According to HHS, "The bottom line is that the costs authorized by the State must be those that are permitted by the HIPAA Privacy Rule and must be reasonable. The HIPAA Privacy Rule at 45 CFR 164.524(c)(4) permits a covered entity to charge a reasonable, cost-based fee that covers only certain limited labor, supply, and postage costs that may apply in providing an individual with a copy of PHI in the form and format requested or agreed to by the individual. Thus, labor (e.g., for search and retrieval) or other costs not permitted by the Privacy Rule may not be charged to individuals even if authorized by State law. Further, a covered entity's fee for providing an individual with a copy of her PHI must be reasonable in addition to cost-based, and there may be circumstances where a State authorized fee is not reasonable, even if the State authorized fee covers only permitted labor, supply, and postage costs. For example, a State-authorized fee may be higher than the covered entity's cost to provide the copy of PHI. In addition, many States with authorized fee structures have not updated their laws to account for efficiencies that exist when generating copies of information maintained electronically. Therefore, these State authorized fees for copies of PHI maintained electronically may not be reasonable for purposes of 45 CFR 164.524(c)(4)."

IT IS HELPFUL TO KEEP IN MIND THE GENERAL PRINCIPLE UNDERLYING HIPAA'S HEALTH INFORMATION RIGHT OF ACCESS:

Whichever provision, federal or state, that gives a patient a greater right of access or greater protection of the privacy of their health information is what will govern.

OHIO LAW:

TOTAL COSTS FOR COPIES AND ALL RELATED SERVICES IN OHIO SHALL NOT EXCEED THE FOLLOWING:

Click here for the 2022 Medical Price Index. Copying fees are usually available in late January or early February and could go up or down based on the CPI.

1. Requests Made by a Patient(s) or a Patient's Personal Representative
   a. Paper Records
      i. $3.51 per page for the first 10 pages
      ii. $0.73 per page for pages 11-50
      iii. $0.29 per page for pages 51 and above
      iv. The actual cost of any related postage incurred
   b. All Other Recorded Data (i.e., X-rays, MRIs, EKG strips)
      i. $2.41 per page
      ii. Postage

2. Requests by Others
   a. Paper Records
      i. Initial fee of $21.65
      ii. $1.42 per page for the first 10 pages
      iii. $0.73 per page for pages 11-50
      iv. $0.29 per page for pages 51 and above
      v. Postage
   b. Data resulting from an X-ray, MRI, or CAT scan recorded on paper or film
      i. $2.35 per page
      ii. Postage

The maximum charges are adjusted annually to reflect the average percentage of increase or decrease in the Consumer Price Index (ORC Section 3701.741).

THERE ARE SOME EXCEPTIONS AND EXEMPTIONS TO THESE CHARGES UNDER OHIO LAW.

1. Physicians and medical records companies may enter into a contract with a patient, a patient's personal representative, an authorized person or a health insurer for the copying of records at a fee that differs from statutory maximums.

2. Maximum statutory charges do not apply to medical records of long term care residents accessed by the long term care ombudsman (ORC Section 173.20) or medical records requested by long term care residents or their legal representatives (42 CFR Section 483.10).

3. The Bureau of Worker's Compensation and the Department of Job and Family Services are entitled to one free copy of a medical record. A patient (or his personal representative) is also entitled to one free copy of a medical record if it is necessary to support a claim for Social Security Disability or Supplemental Security Income. This request must also be accompanied by documentation a claim has been filed.

TIMEFRAME FOR RESPONDING TO REQUESTS

Although Ohio law does not specify a particular timeframe within which to respond to a request, a provider must permit the patient to examine the records or provide a copy of the records "within a reasonable time after receiving the request." If a provider fails to provide a copy of a requested record, the requestor may file a civil suit to enforce their right of access to the record.

HIPAA provides for more stringent guidelines – upon receiving a request for records, a provider must take action in 30 days and is allowed one 30 day extension. If the provider must use this extension, the reasons for its delay must be provided to the patient in writing and the date by which the request will be completed.

BEST PRACTICE TIP

See AMA Ethical Guidance on Medical Records at:

www.ama-assn.org/delivering-care/ethics/code-medical-ethics-privacy-confidentiality-medical-records

DISCLOSURE OF PROTECTED HEALTH INFORMATION (PHI)

It is imperative practices implement policies and procedures that reduce the unnecessary disclosure of PHI to comply with HIPAA. The release of PHI falls under three categories: permissive disclosure, mandatory disclosure and authorization.

PERMISSIVE DISCLOSURE

A permissive disclosure is the release of PHI for the purpose of treatment, payment or health care operations (TPO). This type of disclosure is common and occurs in the day to day practice of medicine. TPO is defined below.

1. **TREATMENT:** the provision, coordination or management of healthcare and related services by one or more health care providers, including referral of a patient from one provider to another or consultation between providers about a patient.
2. **PAYMENT:** encompasses numerous activities of a health plan to obtain premiums, fulfill its coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provision of healthcare. It also encompasses activities of health care providers to obtain payment or be reimbursed for services.
3. **HEALTH CARE OPERATIONS:** administrative, financial, legal and quality control activities necessary for a practice to run its business and support its treatment and payment functions.

Assuming the communication of PHI relates to TPO and proper policies and procedures are in place, a practice may make permissive disclosures to another practice, physician, etc. Patient involvement is not necessary. However, patients may request to limit the disclosure of their PHI relating to TPO. Physicians may refuse to abide by certain requests. However, physicians are required to abide by a patient request to not release information about care the patient has paid for out-of-pocket to health plans, if for treatment purposes, unless the disclosure is required by law.

MANDATORY DISCLOSURE

A mandatory disclosure is a disclosure of patient information required by either Ohio or federal law. As the list below indicates, the government does have extensive access to patient records.

MANDATORY DISCLOSURES INCLUDE:

1. Suspected child abuse (ORC Section 2151.421), adult abuse or elder abuse (ORC Section 5101.61);
2. Suspected abuse of a mentally retarded, developmentally disabled or physically impaired person under the age of 21;
3. Gunshot wounds, stab wounds, burn injury or death (ORC Section 2921.22);
4. Some types of state and federal governmental investigations;
5. Federal laws that require reporting drug complications to the FDA; and,
6. Court orders, subpoenas or other requests pursuant to Ohio law.

HIPAA AUTHORIZATIONS

Sometimes a patient's PHI must be released under a HIPAA compliant authorization. Any release of information that is not a permissive or mandatory disclosure per HIPAA guidelines must be released under a HIPAA compliant authorization that must include the following (45 CFR Section 164.508(c)).

1. Description of the PHI to be released;
2. Who is authorized to make the disclosure;
3. Who may receive the PHI;
4. Purpose for the disclosure;
5. When the authorization expires;
6. Signature and date;
7. A statement notifying the patient of the right to revoke the authorization;
8. Notification to the patient that the physician has no control over the rerelease of information once it leaves the practice's office; and,
9. A statement notifying the patient that under most circumstances treatment is not dependent on the patient signing the authorization.

BEST PRACTICE TIP

In 2019, Ohio adopted a standard authorization form that anyone may use for the release of PHI requiring an authorization. All entities must accept this form as a valid authorization for the use and disclosure of PHI.

Access the instructions at:
https://medicaid.ohio.gov/Portals/0/Providers/SAF/SAF.pdf

And the form at:
https://medicaid.ohio.gov/Portals/0/Resources/Publications/Forms/ODM10221fillx.pdf

RESPONDING TO CIVIL SUBPOENAS

A subpoena is a legal document used to compel the attendance of a witness and/or the production of specified items at a deposition or judicial proceeding. Generally, a subpoena is issued by a court reporter, a notary public or an attorney.

TO BE A VALID SUBPOENA UNDER OHIO CIVIL RULE OF PROCEDURE 45, IT MUST:

1. State the style of the suit and its case number;
2. State from which court the subpoena was issued;
3. Identify the person(s) to whom the subpoena is directed;
4. State the time, place and nature of the action required by the person to whom the subpoena is directed (See Ohio Civ. R. (A)(1)(b)(i) – (vi));
5. State the text of Ohio Rules of Civil Procedure 45(C) and (D) (which discuss enforcement of subpoenas);
6. Signature of the issuing party; and,
7. Prompt, written notice must accompany the subpoena.

BEST PRACTICE TIP

DO NOT IGNORE A SUBPOENA! If there is a question as to the validity of the subpoena, timely contact legal counsel for questions about whether the subpoena is valid as well as best practices for response.

RESPONDING TO CRIMINAL SUBPOENAS

Subpoenas may also be issued in criminal proceedings. Likely, the subpoena will request patient records or request the presence of a physician at trial. Under Ohio law, physician-patient confidentiality is recognized. However, this confidentiality privilege can be waived by the patient. It also does not apply to records requested by law enforcement as part of a criminal investigation relating to alcohol or drug tests.

RIGHTS OF OTHERS

While HIPAA and Ohio law require health care providers to protect patient privacy, there are instances when a patient's medical records may be accessed by someone other than the patient if the patient agrees or other law permits access.

1. **SPOUSES:** absent explicit permission, spouses cannot see each other's medical records.
2. **ADULT CHILDREN:** an adult child cannot see an elderly parent's medical records unless the parent has signed a release form or the parent is incompetent. The parent may already have a durable power of attorney for health care in place (See ORC Section 1337.13). The provider may choose not to recognize that a person's health care power of attorney, however, in the exception that the provider, in the exercise of professional judgement, has a good faith concern or reasonable belief that:

- the individual has been or may be subject to abuse, neglect, or domestic violence by the personal representative possessing the power of attorney,
- recognizing this person's power of attorney endangers the individual,
- treating this person as the personal representative of the individual with power of attorney is not in the individual's best interest.

3. **DECEDENTS:** providers are permitted to disclose a decedent's PHI to family members and others who were involved in the care or payment for care of the decedent prior to death, and the provider is unaware of any expressed preference to the contrary. This disclosure is permitted, not required, so if a provider questions a relationship or does not feel a disclosure is appropriate under the circumstances, he does not have to disclose information. Please be aware—a decedent's PHI is protected for fifty (50) years after death in the same manner and to the same extent as a living person. A deceased individual's legally authorized executor, administrator or someone otherwise legally authorized to act on behalf of the deceased individual or his or her estate may obtain the decedent's health information or provide the appropriate authorization for obtaining it.

   - ***EXAMPLE:*** a provider is permitted to disclose billing information to a family member of a decedent who is assisting with wrapping up the decedent's estate.
   - ***EXAMPLE:*** a provider is permitted to describe the circumstances that led to an individual's passing with the decedent's sister who is asking about her sibling's death.
   - ***EXAMPLE:*** a provider is permitted to release the decedent's health care information to a health care provider treating a surviving relative for treatment purposes.

4. **DIVORCED/SEPARATED PARENTS:** both parents have access to a child's medical records, unless there is a court order which states otherwise (ORC Section 3109.051). For more information regarding the treatment of minors and the rights of divorced parents, please see the ***OSMA Legal Brief — Treating Minors***, or contact the OSMA.

SECTION 4

NOTICE OF PRIVACY PRACTICES

A Notice of Privacy Practices (NPP) is a document that gives reasonable notice of how and when a patient's PHI will be used, the patient's rights and the physician's legal duties regarding PHI (45 CFR 164.520(a)). At a minimum, a NPP must include information about the practice's policies and procedures, detail patients' rights and inform patients whom in the practice they can contact to lodge a privacy complaint or to receive further information.

The NPP must be written in plain language and contain the date of the notice. HIPAA requires the following header language to be displayed in all capital letters.

> **THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY. (45 CFR SECTION 164.520(B)(I)).**

POSTING THE NOTICE

The NPP must be prominently displayed within the practice in its entirety. The displayed NPP must be in a place where it is reasonable to expect patients will be able to read it—most likely the waiting room. The practice is required to provide the NPP to every new patient and anyone else on request. If the practice maintains a website, the NPP must be posted on the website and available for download.

BEST PRACTICE TIP

The displayed NPP must be in a place where it is reasonable to expect patients will be able to read it—most likely the waiting room.

PATIENT ACKNOWLEDGEMENT

Each patient must provide written verification that he or she was provided a copy of the practice's NPP, unless in an emergency treatment situation. This verification does not require that the patient has read and understands the notice. If a written verification is not obtained, the practice must document its good faith attempt to obtain a written verification and why it was not obtained. If the notice is provided electronically to a patient, the written acknowledgment may be in the form of an electronic return receipt or other return transmission.

MATERIAL CHARGES

Practices may have to revise the NPP from time to time to include any necessary, material changes. The revised NPP must be posted in the office and posted on the practice's website. Copies of the revised NPP must be available at the office to all new patients and to any other patients upon request.

OTHER REQUIRED INFORMATION

THE FOLLOWING ADDITIONAL INFORMATION MUST BE INCLUDED IN A PRACTICE'S NPP:

1. A description of at least one example of the types of uses and disclosures the practice is permitted to make for TPO;
2. A description of the other purposes for which the office is permitted or required to disclose PHI without patient consent or authorization;
3. A description of the types of uses and disclosures that require the patient's authorization and a statement that other uses and disclosures not described in the notice will be made only with the individual's written authorization;
4. The practice may contact a patient for fundraising purposes and the patient has the right to opt out of receiving such communications;
5. A statement that the patient has a right to request restrictions on certain uses and disclosures of PHI, including a statement that the practice is not required to agree to a requested restriction, unless the request restricts the disclosure of PHI relating to care the patient has paid for out-of-pocket in full to health plans;
6. A statement that the practice is required to maintain the privacy of PHI, to provide patients with notice of its legal duties and privacy practices with respect to PHI, and to notify affected patients following a breach of unsecured PHI;
7. A statement that the practice is required to abide by the terms of the NPP, that the practice reserves the right to revise the NPP and a description of how the revised copy will be provided;
8. Include information about how patients may obtain copies of their records and what fees, if any, will be charged;
9. A statement of how the patient may complain about the practice to the Secretary of HHS and notification the practice will not retaliate against the patient for filing a complaint;
10. The right to inspect, copy and amend PHI;
11. The right to receive a paper copy of the privacy notice;
12. The right to receive an accounting of PHI disclosures made not pursuant to a HIPAA authorization or for a purpose other than TPO; and,
13. The right to receive confidential communications by alternative means or at alternative locations.

REMEMBER:

The NPP must be written in plain language and contain the date of the notice. HIPAA requires the header language to be displayed in all capital letters.

SECTION 5

ADDITIONAL HIPAA COMPLIANCE & APPLICABLE OHIO LAWS

THE HIPAA FINAL OMNIBUS RULE WAS PROMULGATED ON JAN. 25, 2013 TO STRENGTHEN THE PRIVACY AND SECURITY PROTECTION FOR AN INDIVIDUAL'S PHI. OHIO HAS STATED AN INTENT TO MAKE OHIO LAW AND HIPAA CONSISTENT AS IT APPLIES TO ELECTRONIC MEDICAL RECORDS AND HEALTH INFORMATION EXCHANGES. SEE OHIO REVISED CODE SECTIONS 3798.01 THROUGH 3798.16.

WHO IS COVERED

HIPAA applies to all "covered entities." A covered entity is defined in the rule as a health plan, a health care clearinghouse or a health care provider that transmits health information electronically.

BUSINESS ASSOCIATE AGREEMENTS

A business associate agreement (BAA) is a contract a provider enters into with an outside individual or company who performs services or activities on behalf of the provider. The BAA imposes specified written safeguards on PHI to be used or disclosed by the business associate. A business associate may include organizations involved in billing or practice management, or that provide legal, financial or consulting services requiring PHI. Although many HIPAA provisions apply directly to business associates (and the obligation to enforce these rules with respect to business associate subcontractors), a practice must be very careful to thoroughly screen any outside vendor it is considering doing business with in order to remain HIPAA compliant.

BEST PRACTICE TIP

Consult legal counsel to draft a BAA specifically tailored for use in your practice. Exercise caution and thoroughly review a BAA provided by a business associate.

PRIVACY POLICIES & PROCEDURES

A practice must put in place certain safeguards to protect PHI and minimize its use and disclosure. Practices must:

1. Take reasonable measures to protect PHI from unnecessary disclosure;
2. Develop and implement policies and procedures which reduce the inappropriate or unnecessary disclosure of PHI;
3. Designate a privacy officer to oversee the adoption of privacy procedures; and,
4. Train all workforce members on its privacy policies and procedures.

BREACH NOTIFICATION RULE

Covered entities are required to notify affected individuals following the discovery of a breach of unsecured PHI. "Unsecured" PHI is PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons by means of an approved methodology such as encryption. (See 45 CFR Section 164.404) A ''breach'' means the unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of such information. Breaches are presumed reportable unless, after completing a risk analysis applying four factors, it is determined there is a low probability of PHI compromise. The four factors are:

1. Nature and extent of the PHI involved;
2. The person who obtained the unauthorized access and whether that person has an independent obligation to protect the confidentiality of the information;
3. Whether the PHI was actually accessed or acquired, after conducting a forensic analysis; and,
4. The extent to which the risk has been mitigated.

REMEMBER:

For breaches involving 500 patients or more, the Secretary of HHS must be notified contemporaneously with affected patients.

ACTUAL REPORTING & TIMEFRAME REQUIREMENTS

If a breach has occurred, all affected individuals must be notified without unreasonable delay and not later than 60 calendar days following the discovery of the breach, unless otherwise directed by law enforcement. For breaches involving 500 patients or more, the Secretary of HHS must be notified contemporaneously with affected patients. Prominent media outlets serving the state or jurisdiction must also be notified. For breaches involving 500 patients or less, the names must be logged and reported to HHS annually.

CIVIL PENALITIES AND HIPAA VIOLATIONS

HIPAA violations by a practice may very well lead to monetary penalties. A four (4) tier penalty system is in place, with increasing levels of culpability.

HHS must conduct a formal investigation and impose civil monetary penalties in cases involving willful neglect. HHS may provide PHI to other government agencies for enforcement activities.

THE ASSESSMENT OF PENALTIES IS BASED ON FIVE (5) FACTORS.

1. The nature and extent of the violation, including the number of individuals affected;
2. The nature and extent of the harm resulting from the violation, including reputational harm;
3. The history and extent of prior compliance;
4. The financial condition of the covered entity or business associate; and,
5. Such other matters as justice may require.

The number of violations may be based on the number of individuals affected or by the number of days where the practice was non-compliant.

In the case of willful neglect, HHS not only presumes actual or constructive knowledge a violation is certain to occur, but also that a provider consciously intended or acted recklessly regarding his compliance obligations. An example of willful neglect is an employee of a medical practice losing an unencrypted laptop containing PHI and an HHS investigation reveals the practice failed to notify affected patients of the breach. The rules provide a “cure period” of 30 days to correct a violation in the case of willful neglect. This period begins when the physician knew, or would have known by exercising reasonable diligence, a violation occurred.

CRIMINAL PENALITIES UNDER HIPAA

Criminal penalties are imposed when a patient’s privacy is intentionally violated for malicious or fraudulent reasons, or for personal financial gain.

SECTION 6

AMENDMENT OF RECORDS

HIPAA provides a patient the right to amend his or her medical record. (45 CFR Section 164.526). This right to amend is limited. A patient may add more information to a medical record, but this right does not extend to changing, removing or altering information that is already in the record.

TIMEFRAME

If a provider does accept a patient's request to amend, the amendment must be made no later than 60 days after receipt of the request. Should the provider be unable to make the amendment within this 60-day timeframe, it may have one 30-day extension provided that it informs the patient during this time period in writing the reason for the delay and the date by which the amendment will be made.

DENIALS

A provider can deny a patient's request for an amendment. Denials can be made when a provider did not create the record the patient wants to amend or if the record is complete and accurate. Denials must be in writing.

THERE ARE TWO TYPES OF DENIALS:

1. Denial with No Review: patients have no right to amend records they had no right to access in the first place. For example, a patient may not request to amend records maintained in anticipation of legal action.
2. Denial with Right to Review: a physician may deny a patient's request to amend but the patient will have the opportunity to appeal this decision.

Amendments become a part of the patient's medical record. The amendments should be clearly labeled, regardless of whether the records are paper or electronic.

REMEMBER:

Use caution when denying a request to amend. The denial process can be lengthy and the patient can file a complaint with the government if his or her request to amend is denied.

SECTION 7

RETENTION, STORAGE, TRANSFER, SAFEGUARDS & DESTRUCTION

RETENTION

Proper retention of medical records is often a common point of confusion for many medical practices and physicians. While Ohio does not have a specific statute which requires the retention of medical records for a minimum period of time, there are a number of federal and Ohio statutes that do provide guidance when determining how long to retain medical records.

1. **OHIO STATUTES OF LIMITATIONS:** All medical records should be retained for at least a length of time equal to the statute of limitations associated with the type of treatment provided. An action for medical malpractice must typically be commenced within one year after the action accrues. (ORC Section 2305.113). However, the action accrues when the injury should have been or is discovered. There are exceptions to this one year statute, including, a two-year statute of limitations for wrongful death actions and the tolling of the statute until the age of majority, for the treatment of a minor. (ORC Section 2305.16).
2. **MEDICARE AND MEDICAID:** The federal statute of limitations sets a limit of six (6) years on fraud cases. (45 CFR Section 1003.132) Ohio law also mandates that a health care provider retain all records dealing with the treatment of a Medicaid patient for at least six (6) years. (ORC Section 2913.40(D)). Finally, as a condition of participation in the Federal Medicare Program, providers agree to retain all medical records dealing with the treatment of a Medicare patient for at least five (5) years.

For additional information, see AMA Code of Ethics, Chapter 3, Opinions on privacy, confidentiality and medical records, accessible at: ***ama-assn.org***

BEST PRACTICE TIP

A case-by-case evaluation should be conducted when determining how long medical records should be retained under the statute of limitations criteria.

BEST PRACTICE TIP

A practice should adopt a Records Retention Policy prior to any destruction of records. Whenever possible, records should be retained indefinitely. If a record must be destroyed, do so in a confidential manner and consider other ethical and legal ramifications. When in doubt, please contact an attorney to help make this determination.

STORAGE

Issues regarding the storage of medical records typically arise when a physician plans to retire. It is imperative a physician make provisions for the proper handling and storage of medical records. It is common practice to name a custodian of the records whether that is the practice the physician is leaving, another physician or a commercial records management service.

TRANSFER OF RECORDS

No medical records, copies of records, summaries of records or other information contained within a patient's medical record may be transferred without the patient's prior written permission. In any event of transfer of records, patients should be notified that they may obtain a copy of their records or designate a physician to receive their records.

BEST PRACTICE TIP

If a physician chooses to transfer patient records to a custodian, it is recommended a contract be written requiring the custodian to notify the physician if he moves or no longer wishes to maintain the records. This is known as a custodial agreement.

SAFEGUARDS

HIPAA requires all appropriate administrative, technical and physical safeguards be applied to protect the privacy of medical records and other PHI. Please refer to 45 CFR Section 164.530(c).

DESTRUCTION

HIPAA requires records containing PHI be disposed of in such a manner that renders the PHI unusable, unreadable or indecipherable to unauthorized individuals. (45 CFR Section 164.402(2)(iii). As such, providers must implement policies and procedures to address the final disposition of all PHI, including electronic PHI. Providers' staff must receive training on these disposal policies. HIPAA does NOT require a particular disposal method.

PROPER DISPOSAL METHODS INCLUDE:

1. **Paper PHI:** shredding, burning, pulping or pulverizing.
2. **Electronic PHI:** permanently destroying/erasing PHI from the media.
3. **Labeled Prescription Bottles/Other PHI:** place in a secure area in opaque receptacles for disposal by a disposal vendor as a business associate.

To prevent the accidental destruction of medical records from occurrences such as a fire or a natural disaster, keep an electronic backup of records or store paper copies offsite.

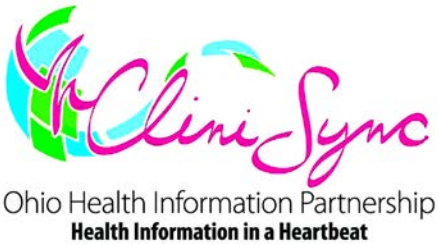
BEST PRACTICE TIP

NEVER destroy a medical record involved in any legal matter which has not been resolved.

HEALTH INFORMATION EXCHANGES

An electronic health information exchange (HIE) allows doctors, nurses, pharmacists, other health care providers and patients to appropriately access and securely share a patient's vital medical information electronically between health care providers— improving the speed, quality, safety and cost of patient care. The goal of HIE is for information to follow patients, wherever and whenever they seek care, in a private and secure manner. ***CliniSync*** is Ohio's statewide HIE. While some physicians, hospitals and healthcare professionals use EHRs strictly within their own facilities or exchange patient information regionally or within a health system, this exchange is statewide. Once a practice has changed to an EHR system, it would be worthwhile to consider connecting to an HIE system such as ***CliniSync***. For further information regarding ***Clinisync***, please visit ***www.clinisync.org***.

(Note that the OSMA is a founding partner of the Ohio Health Information Partnership.)



HELPFUL TOOLS & WEB RESOURCES:

American Academy of Family Physicians Closing a Medical Practice
https://www.aafp.org/dam/AAFP/documents/practice_management/admin_staffing/ClosingPracticeChecklist.pdf

HIPAA Final Omnibus Rule: Summary, Modifications and Comments
http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

List of Forbidden Abbreviations
www.jointcommission.org/facts_about_do_not_use_list

Medicare and Medicaid Incentive Programs
www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Basics.html

Office of the National Coordinator for Health Information Technology
www.healthit.gov

Ohio Administrative Code
http://codes.ohio.gov/oac

Ohio Health Information Partnership
www.clinisync.org

Ohio Revised Code
http://codes.ohio.gov/orc

Ohio State Medical Association Telehealth Webpage
www.osma.org/telehealth

To Obtain a Sample Notice of Privacy Practice (NPP)
www.hhs.gov/ocr/privacy/hipaa/modelnotices.html

To Obtain a Sample Business Associate Agreement (BAA)
www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html

The Doctors Company Frequently Asked Medical Records Questions
www.thedoctors.com/articles/medical-records-and-documentation

U.S. Department of Health & Human Services – HIPAA FAQs
www.hhs.gov/hipaa/for-professionals/faq

U.S. Department of Health & Human Services – HIPAA Regulation Text
www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text

Ohio State Medical Association

Bringing physicians together for a healthier Ohio

OUR MISSION

OSMA IS DEDICATED TO EMPOWERING PHYSICIANS, RESIDENTS & MEDICAL STUDENTS TO ADVOCATE ON BEHALF OF THEIR PATIENTS, COMMUNITIES & PROFESSION.

VISIT

www.OSMA.org

5115 Parkcenter Avenue
Suite 200
Dublin, OH 43017

Toll-free: (800) 766-6762
(614) 527-6762
Fax: (614) 527-6763
info@osma.org