Indiana University Health

HIPAA FAQ – Protecting Patient Privacy

Patient privacy and protection of confidential patient health information (PHI) is essential to the care IU Health provides. Accessing patient information in an electronic medical record (EMR) or other systems (e.g. Cerner, Epic, PACS) without an authorized need is a violation of IU Health's privacy policies.

As an added safeguard to keeping patient information confidential and secure, the Privacy Office launched a new, automated auditing tool in February 2018 called Haystack. Since then, the Privacy team has used Haystack to keep track of EMR activity across IU Health.

In the event Haystack flags an out-of-the-ordinary behavior based on a team member's previous activities, job codes and other factors, the Privacy Office is alerted to investigate. If a privacy violation is found to have occurred, this will result in the appropriate disciplinary action, including restricting access to the EMR and termination of employment.

As caregivers and team members, we sometimes don't realize that casually looking up or relaying information about patients to other team members, physicians or providers can result in a HIPAA incident.

Please carefully review the following answers to frequently asked questions to learn more about HIPAA requirements and real-world scenarios we often face.

Understanding the Basics of Protected Health Information (PHI)

Q: **What is considered protected health information (PHI) requiring HIPAA confidentiality, privacy and security protections?**

A: PHI includes an individual's past, present or future medical treatment as well as **any** information that would identify a patient. In addition to a patient's medical treatment, HIPAA sets forth 18 identifiers that constitute PHI and all are entitled to HIPAA confidentiality protections:

- First, last and middle names
- All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code and their equivalents geocodes
- All elements of dates (except year) for dates that are directly related to an individual, including birth date, admission date, discharge date, death date and all ages over 89 and all elements of dates (including year) indicative of such age

- Telephone or fax numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Email addresses
- Web Universal Resource Locators (URLs), including social media profiles
- Social Security numbers
- Internet Protocol (IP) addresses
- Medical record numbers
- Biometric identifiers, including finger and voice prints
- Health plan beneficiary numbers
- Full-face photographs and any comparable images
- Account numbers
- Any other unique identifying number, characteristic or code
- Certificate/license numbers

Q: Can I send protected health information (PHI) via text message on my cell phone, pager or other device?

A: No. Text messages or pages are not secure. The Diagnotes application, which may be downloaded from the App Store, is the only IU Health-approved secure and encrypted method for sending PHI electronic messages. Use your IU Health log-in credentials to access Diagnotes where electronic messages from provider to provider or team member to team member may occur in a secure environment, including the sending of photographs and videos via Diagnotes.

Q: Can I send protected health information (PHI) via email?

A: If you need to send PHI via email for legitimate IU Health business reasons (e.g. treatment, payment, health care operations), then you may send PHI via email from an IU Health email account to another IU Health email account. In addition, PHI may be sent via email from an IU Health email account to an IU Faculty, Resident, Fellow or Medical Student email account or an Eskenazi email account as we have secured these communications.

If you are sending PHI to a non-IU Health/non-IU Faculty, Resident, Fellow or Medical Student/non-Eskenazi email account (e.g. Gmail, Yahoo, Comcast, AOL, etc.), then you must place *only* the words "*Secure Message"* in the Subject line of the email to direct our systems to encrypt the email to send PHI securely via email outside of IU Health.

NOTE: Indiana University undergraduate and graduate student email accounts are not approved for transmission of PHI unless otherwise specified above.

Q: Can I engage in physician-patient email conversations?

A: Yes, but only if you:

- Have the patient's signed *Patient Email Usage Consent* form in advance

- Send the email in a secure, encrypted fashion (see above)
- Maintain email communications pertinent to the ongoing care of the patient as part of the patient's medical record.

This is required by Indiana Professional Licensure Rules and under HIPAA compliance. Instead of physician-patient email, it is recommended that patients be referred to the Patient Portal at **MyIUHealth.org** to send messages to your care team (*HIPAA 3.20, 844 IAC 5-3-4 and 844 IAC 5-3-5*).

Q: Am I allowed to discuss protected health information during patient check-in or check-out at a physician office visit?

A: Yes, as long as you are exercising reasonable safeguards. Under HIPAA, everyone is required to exercise reasonable safeguards to protect our patients' confidential PHI. This may include:

- Speaking in a lowered voice at patient check-in
- Moving the patient to a private area if you need to discuss a sensitive matter
- Asking patients to sit down rather than standing in a long line at patient check-in where conversations could be overheard
- Asking a patient to write down their social security number rather than verbalizing
- Always double checking that you're giving the correct patient the correct discharge summary, documentation and/or prescription
- Ensuring that your computer screen is not publicly visible or use a computer privacy shield/screen (*HIPAA 2.01*)

Accessing Health Records for Personal Interest

Q: Can I access and view my own health records in the Cerner electronic medical record (EMR) or other systems containing PHI?

A: No. To protect the integrity and confidentiality of all health records you should never access your own health records through the Cerner EMR or any other system containing PHI.

To view your own health records, you should visit the Patient Portal at **MyIUHealth.org**, request a copy from Health Information Management or discuss your care with your provider (*IS Policy 1.29*). Using your provider/user credentials to access the Cerner EMR is permitted under HIPAA for your *treatment of patients*, *payment* and *health care operations*. It is not permissible to access the Cerner EMR for personal reasons (*HIPAA Policy 2.11*).

Q: I am a parent of minor child and/or an Authorized Representative under a medical Power of Attorney over my spouse. Can I access and view my child's or spouse's health records in the Cerner electronic medical record (EMR) or other systems containing PHI?

A: No. To protect the integrity and confidentiality of all health records you should not access your child's or spouse's health records through the Cerner EMR or any other system containing PHI.

While parents are generally entitled to the PHI of their minor children and an Authorized Representative under a medical Power of Attorney is entitled to PHI, you may **not** directly access this information in the Cerner EMR. Visit the Patient Portal at **MyIUHealth.org**, request a copy from Health Information Management, or discuss your care with your provider (*IS Policy 1.29*).

Using your provider/user credentials to access the Cerner EMR is permitted under HIPAA for your *treatment of patients*, *payment* and *health care operations*. It is not permissible to access the EMR for personal reasons (*HIPAA Policy 2.11*).

Q: **My mother-in-law is a patient and I am visiting her. She is asking me questions that I can find out for her by logging into the Cerner electronic medical record (EMR). Can I look in Cerner?**

A: No. You are not part of the care team treating your mother-in-law, so you should *not* access and view her health records in Cerner, even to provide your mother-in-law with medical information. Instead, please assist your mother-in-law by having someone on her care team provide the information she needs.

Q: **My co-worker was just transported via ambulance to an IU Health Emergency Department and out of concern for her well-being I want to quickly look into her status through the Cerner electronic medical record (EMR) just to make sure that she will be ok. Can I do this?**

A: No. You should not access and view health records through the Cerner EMR for family members, friends, neighbors, co-workers or others unless you have a legitimate IU Health business reason to do so (e.g. you are performing treatment, payment, health care operations). Accessing and viewing your co-worker's Emergency Department visit in the EMR out of concern is not a legitimate IU Health business reason.

Q: **The local news reported that my favorite Indianapolis 500 race car driver was transported to an IU Health facility. I am a longtime race fan and am curious to see how serious his injuries are. I will not disclose the driver's treatment to anyone. Can I access the driver's Cerner electronic medical record (EMR) to take a quick look as long as I don't share what I viewed with anyone else?**

A: No. It is never permissible to look at the medical information of friends, family, colleagues, celebrities or high-profile patients out of curiosity. You should not access and view health records unless you have a legitimate IU Health business reason to do so (e.g. you are performing treatment, payment, health care operations).

Q: **I volunteer for every year at a local high school and give an overview of healthcare careers in the field of Radiology. I found an interesting ultrasound that I would like to show the students. Can I do this?**

A: Not unless you have removed all protected health information (PHI) from the ultrasound in accordance with the *De-Identification of Protected Health Information Policy* (*HIPAA 7.06*). Once an ultrasound image has been de-identified in accordance with HIPAA by the removal of 18 identifiers and cannot otherwise be tied to a patient, it is no longer deemed PHI.

Accessing Health Records for Professional Interest

Q: **I am a new nurse, and I am eager to learn about all types of health conditions. In between patients, can I search the Cerner electronic medical record (EMR) for unique health conditions that I might encounter in the future?**

A: No. A team member may not self-initiate a random search through the EMR to look for interesting health conditions. In this instance, the team member should discuss with their manager appropriate opportunities for learning.

Q: **I am a Resident, and I need to access protected health information (PHI) as part of my training program to complete a case study. Can I access PHI in the Cerner electronic medical record (EMR) for this purpose?**

A: Yes, with limitations. HIPAA permits use of PHI for "conducting training programs in which students, trainees or practitioners in areas of health care learn under supervision to practice or improve their skills as healthcare providers." While HIPAA permits the sharing of PHI for education/training purposes, there are limitations on those accesses, uses and disclosures. Enhanced HIPAA Training guidance for Learners/Faculty is under development and will be published in the near future.

Q: **I am the on-call anesthesiologist and a trauma activation has been called in the Emergency Department. I anticipate that I will receive this trauma patient soon in the Operating Room. Can I look at the Cerner electronic medical record (EMR) to see what is occurring with the trauma patient while in the Emergency Department?**

A: Yes. You may view the trauma patient's EMR in anticipation of treatment. As the on-call anesthesiologist, you will be responsible for any anesthesia care. Therefore, for treatment and coordination of care purposes, you can view the patient's activities in the Emergency Department in anticipation of rendering care in the Operating Room, even if circumstances change and you ultimately do not receive the patient.

Similarly, inpatient charge nurses may view the Emergency Department tracking board of their facility in anticipation of legitimately planning for patients to be admitted to their units. It would *not*, however, be permissible to view tracking boards if there is no reasonable basis to believe that a patient would be coming to your unit (e.g. in another facility with capacity to treat; adult patient and you are only treating pediatric patients). It is never appropriate to "snoop" in the EMR.

Q: **I am consulted by a fellow physician on an unusual case. The physician asks for my professional opinion although I am not the attending physician and not directly rendering care to the patient. Can I look at the Cerner electronic medical record (EMR) for this patient?**

A: Yes. As long as you have been legitimately consulted by a physician for a second opinion and/or assistance for treatment purposes, you may access the Cerner EMR on this patient.

Q: **I assist with patients scheduled for surgery and I need to review the Cerner electronic medical record (EMR) to ensure all is in place before the scheduled surgery. Can I continue to do this?**

A: Yes. If you need to access the EMR for patients on your list scheduled for surgery to confirm (e.g., procedure, orders, EKGs, labs, diagnostics, etc.), then you may access the EMR for this legitimate business reason in support of treatment purposes to do your job.

Q: A provider asks me to look into the Cerner electronic medical record (EMR) and to provide confidential protected health information (PHI) on an individual that does not appear to be a patient of the provider. What should I do?

A: Validate that the provider needs access to the PHI for a legitimate IU Health business reasons (e.g., treatment, payment, healthcare operations). You might ask the provider if they are treating the patient, or for what purpose they need access. If in doubt, indicate your discomfort due to patient privacy laws and ask the provider to conduct the search.

Q: I need to quickly check on the status of my patient. Someone else is already logged in to the Cerner electronic medical record (EMR). Can I search the Cerner EMR for my patient without signing in as me?

A: No. It is never permissible to search in the Cerner EMR under the log-in credentials of someone else.

Q: The computer where I document in the Cerner electronic medical record (EMR) is located in a patient room. Can I minimize the screen so patient information is not immediately visible when leaving the computer unattended while logged into the Cerner EMR in a patient room?

A: No. You are *responsible for all activity* under your EMR log-in credentials. Minimizing the computer screen while logged into the Cerner EMR is *not* sufficient as PHI is still accessible. You must always *log out* or *lock your computer* anytime you leave it unattended while logged into the Cerner EMR in public and patient care areas. You can lock your computer by pressing either the *Windows icon + L* or *Control + Alt + Delete* and then clicking *Lock this Computer*. However, if you are using an "auto log-on" computer, you must log out of the EMR when leaving your computer unattended in public and patient care areas (*IS 1.07, IS 1.01*).

Q: I collect quality data for the Critical Care Collaborative. What am I allowed to view within the Cerner electronic medical record (EMR)?

A: Only look at the *minimum necessary* records in the EMR that you have a legitimate IU Health business reason to do so and *need to know* to perform your job duties. For example, if you are collecting data on ICU admissions for the month of October for the purposes of quality improvement by the Critical Care Collaborative, then you would only access the minimum necessary PHI for ICU October encounters and nothing more (e.g., all encounters for the entire year) (*HIPAA 3.10*).

Monitoring Access of Health Records

Q: **Does IU Health monitor who accesses and views patient health records in the Cerner electronic medical record (EMR)?**

A: Yes. IU Health regularly monitors access to the electronic medical record (EMR) systems through Haystack—an automated, proactive EMR software auditing tool used by the Privacy Office. Accessing patient information in an EMR or other system used within IU Health containing PHI leaves an electronic footprint. This footprint provides information on your activity within that medical record or system. The Privacy Office uses this footprint to monitor who is accessing a patient's medical record and/or your access into records.

Q: How is Haystack used?

A: If a concern is raised about access into a medical record, the Privacy Office will investigate. This concern is generally presented via: (i) the system-wide HIPAA reporting (HIPAA@iuhealth.org or 317-963-1940) by team members, patients, visitors or providers; or (ii) daily worklists generated by Haystack, which will flag out-of-ordinary behaviors based on a team member's/provider's previous activities, job codes and other factors.

For example, if a team member who is only responsible for treating minors accesses an adult record, or if a team member who only aggregates patient data for the East Central Region accesses records from the South Central Region, Haystack will flag this behavior. Haystack sends a daily report of all flagged behavior to the Privacy Office, which will evaluate with area management if the access was appropriate.

Q: What happens if my activity is flagged in Haystack?

A: If the Privacy Office cannot substantiate appropriate electronic medical record (EMR) access from the available information, it will send a log of your EMR activity—including a time and date stamp for each click in the EMR—to area management to determine if your access into the EMR was appropriate.

Failure to safeguard the confidentiality our patients' PHI or violation of IU Health HIPAA privacy and security policies may result in disciplinary action, including immediate termination (*HR 100*).

Q: What is the Haystack "self, friends and family" function?

A: The "self, friends and family" function in Haystack will be activated on Nov. 1, 2018 and will specifically monitor whether those given access to the electronic medical record (EMR) are accessing their own records, or those records of close relations or friends. This activity is often called "snooping."

Haystack will use data to detect on a daily basis whether individuals are inappropriately viewing their own EMR, or the EMR of a family member, an acquaintance or a co-worker. If the Privacy Office cannot substantiate appropriate electronic medical record access from information available to it, then area management will be engaged to determine if the access was appropriate.

Failure to safeguard the confidentiality of our patients' PHI or violation of IU Health HIPAA privacy and security policies may result in disciplinary action, including immediate termination (*HR 100*).

Sharing or Storing Personal Health Information (PHI)

Q: **Can I store protected health information (PHI) on a USB flash drive?**

A: Yes, but *only* if the USB flash drive is secure—meaning it is password-protected and encrypted. To obtain an IU Health-approved, password-protected, encrypted USB flash drive, please contact the IS Help Desk at **317.962.2828** or **helpdesk@iuhealth.org**.

Q: **Can I place protected health information (PHI) on a private IU Health Facebook account accessed only by participating team members in my Hospital Department?**

A: No. PHI may not be shared on Facebook or any other social media sites. A "private" Facebook account is never private to the extent required by HIPAA confidentiality provisions.

Q: **Can I use the ShoreTell or Jabber instant messaging systems to discuss protected health information (PHI) with my co-workers?**

A: No. ShoreTell and Jabber are *not* secure and encrypted methods for transmission of PHI and team members may not send PHI via ShoreTell and Jabber instant messages. Presently, IU Health does *not* maintain any instant messaging systems approved for PHI. However, you may download the Diagnotes application, which is approved by IU Health for sending secure and encrypted electronic messages, and is accessible via your IU Health log-in credentials. Diagnotes may also be accessed through Web browsers (e.g. Firefox, Chrome, Internet Explorer) and is approved for use with PHI.

Q: **My leader has approved the use of an online cloud-computing solution for storing electronic protected health information (PHI) used in our outpatient rehabilitation center. How do I engage the online cloud-computing services provider/vendor?**

A: Online cloud-computing solutions take many forms of on-demand internet access to computing (e.g. networks, servers, storage, applications) services that may create, receive, process, maintain or store electronic PHI. First, the cloud services vendor must complete an *IT Risk Assessment Questionnaire* (ITRA), which is to be sent to **ITRA@IUHealth.org**.

IU Health Information Security will review the ITRA and approve moving forward or may require additional security safeguards to be implemented by the vendor. Next, contact your IS Subject Matter expert to submit the Cloud Computing Solution Service Agreement for review and approvals via NTRACTS (IUH's contract approval/repository system). Additionally, all parties are required to enter into a Business Associate Agreement prior to sending any PHI to the cloud services vendor.

Q: **If I receive a suspicious email, what should I do?**

A: Do not click any links in the email. Either click the "Report Phishing" icon in the top right hand corner, or forward the email to infosec@iuhealth.org as soon as possible for a security review.

Reporting a Violation

Q: **How do I report a lost, stolen or compromised personal computer (PC), laptop, system, iPhone, USB flash drive or other device?**

A: Promptly contact the IS Help Desk at **317.962.2828 or helpdesk@iuhealth.org**.

Q: **How do I report a HIPAA complaint or concern, ask a question or report a potential HIPAA breach?**

A: Notify the IU Health Privacy Office via email at **HIPAA@iuhealth.org** or by phone at **317.963.1940**. The HIPAA reporting email and phone number is available to all team members, management, providers, patients and visitors.

Q: **Who makes the determination if the reported incident is a reportable HIPAA breach?**

A: The Privacy Office conducts an investigation into the incident and consults with area management. The Privacy Office may engage IU Health Information Security and Compliance personnel to assist on technical and forensic matters along with other experts. A written risk assessment is completed by the Privacy Office applying the regulatory breach criteria to the facts in order to determine if the incident constitutes a reportable breach. For every reportable breach, the Privacy Office is required by law to notify the patient in writing and to submit a breach report to the Department of Health and Human Services-Office of Civil Rights, which is the federal agency responsible for HIPAA enforcement. The Indiana Attorney General and other agencies may also need to be notified of the breach under certain circumstances.