The PRIVACY QUARTERLY

Volume 3, Issue 1 July 2017

Special points of interest:

- UNC HC: new secure text messaging application
- Search/seizure of pacemaker data in criminal cases
- Epic@UNC: case examples of appropriate access of PHI
- Sensitive PHI: OCR settlement and reminders to use appropriate safeguards

Inside this issue:

UNC Health Care: Text Messaging Appointment Reminders

UNC Health Care recently implemented a secure text messaging application for appointment reminders. If the patient's primary number is a mobile number, for most clinics the patient will receive an automated text message two days prior to a scheduled appointment, instead of a phone call. Patients without a mobile number will still receive a phone call and there are no changes to mailed reminders, recall, and no-show notifications. The texting software identifies what type of phone (mobile or landline) is entered under the patient's "Preferred Number" in Epic. Patients will have the option to confirm or cancel the appointment or to opt-out of text message reminders in the future.

This new technology is only designed to send appointment reminders and is not intended, nor does it represent authorization, to transmit Protected Health Information (PHI) for any purpose other than appointment reminders.

Please click here for more information about secure texting of appointment reminders.

Emerging News: Seizure of Pacemaker Data

An Ohio judge recently ruled that data from a man's pacemaker may be used as evidence against him as he stands trial for aggravated arson and insurance fraud.

The prosecution plans to show that data (such as heart rate and cardiac rhythms) from the suspect's pacemaker before and during a fire is inconsistent with the story he provided to the police. The man told police that he was asleep before the fire, but when he awoke and saw the fire, he hurriedly packed some belongings in a suitcase and bags, broke the glass of his bedroom window with a cane, and threw the bags and suitcase outside before taking them to his car. However, pacemaker data showed that the man was active instead of asleep before the fire and a cardiologist determined that the man's medical conditions would have prevented him from quickly exiting the home with his belongings.

The defense unsuccessfully argued that the pacemaker evidence could not be used at trial because it was obtained through an invalid search warrant and the search/seizure violated the man's constitutional right to privacy. During the execution of the search warrant, the man was compelled to visit a medical center where law enforcement seized information stored on the pacemaker. The prosecution successfully argued that the search/seizure was analogous to other instances where police may permissibly seize medical records and even blood samples for use as evidence in criminal cases.

This case raises interesting questions about how medical data may be used. Depending on the outcome of the case, we may see the judge's decision appealed to a higher court. The Privacy Office will monitor case developments.

In the mean time, please review the UNC Health Care HIPAA Manual's Release of PHI to Law Enforcement Officers (ADMIN 0155) policy.

A New Look for Epic@UNC

Remember: the same UNC Health Care HIPAA policies continue to apply to your Epic access.

With an Epic upgrade in progress across UNC Health Care (UNC HC), this is an opportune time to be reminded of UNC HC HIPAA Manual's *Privacy and Confidentiality of Protected Health Information policy* (ADMIN 0139) requiring that access to protected health information (PHI) be restricted to business need-to-know purposes.

Approved purposes for accessing medical records in Epic include accessing PHI for treatment, payment, and health care operations purposes. Remember, access to PHI for non-business reasons is prohibited. Examples of access for inappropriate purposes include access for: personal reasons (e.g., viewing a spouse's lab results); satisfying curiosity (e.g., reviewing a coworker's records); or public concern (e.g., viewing the records of an athlete, public figure, or other person in the news).

Here are several case examples illustrating when it is permissible and impermissible to access PHI in Epic:

Scenario	Is it Okay to Access the PHI in Epic?	Will Accessing the PHI Violate UNC HC Policy (i.e., there is no appropriate, business need-to-know purpose)?
My neighbor told me that his spouse was admitted to the ER and said I should see if she is doing OK; OR My UNC HC co-worker was in a car accident and admitted to the hospital and I want to find out if he is OK; OR My son, who is 24 years old, is in the hospital and I want to access his records in Epic to see how he is doing.	There are two instances where you may access this patient's medical records: 1. **Direct Access in Epic:** you may access the patient's records directly in Epic ONLY IF: (1) you work in a facility that allows employees to access records directly in Epic and (2) the patient has signed a specific authorization allowing you to access their records in Epic. • Both UNC REX and UNC Hospitals' policies permit employees to access patient records in Epic if the patient signs the appropriate authorization. At REX, please review the On-Line Access of Protected Health Information (2103043) policy. 2. **Paper Copies from HIM:** if you have the patient's written authorization, you may be able to obtain copies of the patient's medical records from Health Information Management (HIM). This does NOT permit you to access the records in Epic.	Unless the patient has signed the Epic specific authorization (available at UNC REX and UNC Hospitals), you may not access the patient's records in Epic.

One of my direct-reports who works for me at UNC HC missed two weeks of work because she said she was sick. I want to access her medical records in Epic to see if she was telling the truth.	No.	This is not an appropriate purpose for accessing an employee's medical records in Epic.
My department is reviewing our clinic's hospital inpatient admission statistics for the last month and I want to pull a report from Epic and/or Business Objects with this information.	This is a permissible business need-to-know purpose and is considered health care operations.	Your access to data and reports should be limited to and list only those data elements necessary for the report.
I am a health care provider and I want to randomly search through Epic to see if I can come across any interesting cases for my own educational purposes.	Access to PHI of your current or former patients or patients who have been seen by you is permissible for educational purposes and/or personal professional development.	However, for patients whom you have not seen or who have been seen outside of your department, you should only access their records in Epic in accordance with UNC HC HIPAA Manual's *Use of PHI for Teaching and Continuous Quality Improvement Purposes policy* (ADMIN 0146). This policy requires that you complete a form to access records for an educational or health care operational purpose of this nature. You may also submit a specific request for these types of records through Business Objects — provided the data identifiers you use to pull your report are narrowly and specifically tailored to your request.

Employee access to patient records in Epic is monitored. Multiple audits are performed to identify and detect inappropriate access by employees to PHI in Epic. Accessing patient information in Epic unrelated to your job may be considered a serious breach of patient privacy. Unauthorized access to a patient's medical record in Epic may result in disciplinary action and possibly termination of employment. Federal law may also require that we notify the patient and federal regulators of the unauthorized access. Remember: it is not worth losing your job because of unauthorized access to PHI in Epic.

Additional information about accessing medical records can be found on our Intranet site.

If you have questions about whether your access to a patient's medical record is authorized under UNC HC HIPAA policies, please contact the Privacy Office prior to accessing the records. You may also share concerns anonymously through the Privacy & Compliance hotline (1-800-362-2921) or incident reporting tool.

The
PRIVACY
OFFICE

James T. Hedrick Building
211 Friday Center Drive
Chapel Hill, NC 27517

Phone: 984-974-1126
Hotline: 1-800-362-2921

Privacy@unchealth.unc.edu

http://intranet.unchealthcare.org/intranet/hospitaldepartments/auditcomplianceprivacy/privacy

Report on Medicare Compliance

Need more Privacy and Compliance information? Please email Melanie.Runge@unchealth.unc.edu to join the weekly *Report on Medicare Compliance* email distribution list and receive PowerPoint updates.

Hospital Pays $378K for Disclosing Sensitive PHI

St. Luke's-Roosevelt Hospital Center (a component of the Mount Sinai Health System) recently agreed to pay $378,000 and enter into a Resolution Agreement with the Office for Civil Rights (OCR) to settle allegations that it violated HIPAA when it faxed medical records to the patient's employer in error. The medical record contained sensitive information concerning HIV status, medical care, sexually transmitted diseases, medications, sexual orientation, mental health diagnosis, and physical abuse.

The patient filed a complaint with OCR, who found that an impermissible disclosure of protected health information (PHI) had occurred. OCR also found that a related breach previously occurred, but St. Luke's-Roosevelt did not address vulnerabilities in its compliance program to prevent impermissible disclosures of PHI. OCR noted: "Individuals cannot trust in a health care system that does not appropriately safeguard their most sensitive PHI. Covered entities [. . .] have the responsibility under HIPAA to both identify and actually implement these safeguards."

So what are safeguards and how do we implement them?

Safeguards are best practices that minimize the possibility of inappropriate use, access, or disclosure of patient information. This is a great opportunity to review safeguards specific to the release of patient records. Before releasing patient records, ask yourself:

1. **Is it part of your role at UNC Health Care to release these records?**
   - Requests for a "full" medical record should always be sent to Health Information Management (HIM) for fulfillment.
   - Not everyone is authorized to release patient information. If you are unsure, discuss it with your supervisor or the Privacy Office prior to the release.

2. **Are you adhering to the minimum necessary standard?**
   - For a release of patient information unrelated to treatment, you should only release the minimum amount of patient information necessary to accomplish the request.
   - If a patient signs a written authorization, never release more than what was authorized. The UNC HC Privacy Authorization for Release of Medical Information form (available in the UNC HC HIPAA Manual on the Intranet) allows patients to specifically authorize the release of sensitive PHI (such as mental health, substance abuse, and HIV/AIDS status records).

3. **Did you double check your information before releasing the records?**
   - Make sure you understand what the patient has asked you to do and confirm that you have an accurate address or fax number.
   - Double check that you have written the correct address on the envelope or entered the correct fax number into the machine.

By implementing safeguards, such as those outlined in this article, you can help ensure that the information you release is compliant with UNC Health Care policies and keep patient information safe from inappropriate disclosure.

Please review relevant policies in the UNC Health Care HIPAA Manual such as: Use & Disclosure of Protected Health Information (PHI) Based on Patient Authorization (ADMIN 0015); Minimum Necessary Standard for Accessing, Requesting and Disclosing PHI (ADMIN 0101); and Privacy/Confidentiality of PHI (ADMIN 0139). At UNC Medical Center, the Facsimile Transmission and Receipt of PHI and Other Confidential Information (ADMIN 0067) and Confidentiality of Patient Information (ADMIN 0026) policies may also be consulted.