



Inside this issue:

UNC HC: FY 2019 Privacy Program Lookback 2

Privacy Tips: Protecting PHI 3

UNC HC Privacy Audits: What is the Patient's Medical Record? 3

Word Scramble: 18 HIPAA Identifiers 4

Privacy Incident Reporting

1-800-362-2921

hotline.unchealthcare.org

Privacy Guidance

984-974-1069

Privacy@unchealth.unc.edu

Five Privacy Reminders to Share at Your Next Staff Meeting

- 1** The “Epic Online Access Form” has not been honored by UNCHCS since Fall 2018! If you at any point completed/submitted an “Epic Online Access Form” to Health Information Management (HIM) to access your own or your family member’s medical record through the Epic system, it is no longer in effect. This access is now considered a violation of UNCHCS policy and is subject to corrective action up to and including termination. To avoid a violation, use My UNC Chart (see next topic).
- 2** Epic is a tool for business/direct patient care and My UNC Chart is for personal use/access to medical records. Please enroll in [My UNC Chart](#) to appropriately access your own Epic medical records at UNC Health Care. Patients may enable “Proxy Access” in MY UNC Chart to share medical records with family members whom they wish to be involved in their care.
- 3** **DO NOT access an Epic medical record for ANY personal reason. Only authorized users with a “Business Need to Know” should access patient records.** A few common examples of personal access violations are:

 - My coworker/family member was in the hospital and I wanted to know their room number and/or see if they are ok.
 - I searched for them because I wanted to look up a coworker’s address or birthdate.
 - I pay for or are involved in my children’s medical insurance and health care.
 - My family member completed a “Limited Release of Information to Family/Friends Form” and I am listed.
 - My family member or coworker told me I could look them up in Epic.
- 4** **The UNCHCS Privacy Office uses advanced software (Protenus) that monitors each access that every workforce member makes in Epic.** The Privacy Office uses this system to determine if a patient’s privacy has been violated. If a member of the UNCHCS workforce is suspected to have accessed protected health information (PHI) inappropriately, the Privacy Office will initiate an investigation. If it is determined that the workforce member has violated UNCHCS HIPAA Policies, they will face corrective action up to and including termination.
- 5** **All updated Privacy policies and forms are on the Intranet for reference by UNCHCS workforce members.** Please review our [Intranet site](#) to ensure compliance regarding use and disclosure of patient information.

UNC Health Care: FY 2019 Privacy Program Lookback

The Privacy Office reviewed our last twelve months of work effort to identify trends to help us set our goals for the year ahead. This past fiscal year (FY 2019), our activities reflected the growth seen throughout UNC Health Care.



Investigations

Our office saw a 47% increase in the number of investigations across UNC Health Care in FY 2019 over FY 2018. Thanks to our access monitoring tool, Protenus, the rate of substantiated cases increased from 65% to 69%. This means that our office is receiving more creditable data on which to initiate an investigation, which in turn allows us to use our limited resources more efficiently.



Corrective Action

When an investigation determines that an employee has violated policy, we recommend corrective action. In FY 2019, 25 employees were terminated across the System for privacy policy violations — an increase from FY 2018 when 14 employees were terminated. The most common corrective action taken as a result of a privacy violation continues to be re-education. In FY 2019, 448 employees were re-educated due to a privacy violation — compared to FY 2018 when 253 employees received re-education. Thankfully, only a small percentage of cases are egregious enough to require employee termination.



Consultations

One popular service that our office provides is staff consultation. Any workforce member may contact our office (984-974-1069 or Privacy@unhealth.unc.edu) to ask a privacy-related question. Our consultations grew in number from 900 in FY 2018 to 1,124 in FY 2019. We encourage all workforce members to contact our office to discuss their privacy questions. We appreciate when workforce members take a privacy-first approach to the issues they face because it minimizes the possibility that a privacy violation will occur.



Training

Privacy training takes many forms at UNC Health Care. New employees learn about our privacy program during new employee orientation and all employees must take annual privacy training. Additionally, Privacy Office staff members are often asked to present at departmental staff meetings across the System. Our staff are always ready to present a general overview of our privacy program and can work with you to develop training focused on a specific topic of concern in your area. In FY 2019, we presented 147 training sessions. To request in-service training for your department, please speak with a member of the Privacy Office team (984-974-1069 or Privacy@unhealth.unc.edu).



Staffing

We expanded our staff in FY 2019 to include a full-time Privacy Program Manager at UNC REX in addition to the Program Manager who is located in Chapel Hill. Two staff members and the Chief Privacy Officer, who are located in Chapel Hill, work across the entire System as needed. Our program is assisted by existing employees at UNC Rockingham Health and Caldwell Memorial.

Thank you to all of the departments who interacted with the Privacy Office last year for a consultation, an investigation, or training event. We appreciate your ongoing support of the UNCHCS Privacy Program and look forward to continuing to assist you this year. How can we assist *your* department? Contact any member of the Privacy Office team by phone or email (984-974-1069 or Privacy@unhealth.unc.edu) to learn more.

Privacy Tips



Spotlight on Protecting PHI

Here are a few important and easy-to-implement tips to help you protect patient privacy and avoid committing a privacy violation:

1. **ACCESSING PHI:** only access the medical information you need to perform your job. Do not access any medical information on friends, family, public figures, or others unless it is for a job-related purpose.
2. **COMPUTER LOG OFFS:** always log off your computer, especially if you use a shared computer or one in a common area where other staff also use the computer.
3. **ENCRYPTION:** ensure that the laptop (or other portable device) you use to store electronic medical information is encrypted. This is especially important if you use a personal laptop.
4. **CLEAR YOUR WORK AREA:** if you work in a clinic or area where there are frequently patients and visitors present, take time to ensure that your work area is clear of patient information.
5. **COMPUTER SCREENS:** if your computer screen is visible to patients and visitors, ensure that you either have a privacy screen installed (so only you
6. **DISCLOSING PHI:** ensure that if you are disclosing medical information to a third party, that third party has the right to that information.
7. **REPORT VIOLATIONS ASAP:** if you experience a privacy violation (such as a lost or stolen device) or an accidental disclosure (such as faxing or emailing medical records to the wrong party), make sure that you notify the UNCHCS Privacy Office as soon as possible. There may be steps we can immediately take to mitigate any harm (such as remotely disabling the device). This will also allow us to notify the patients of any potential harm, as required by state and federal law.

While we have many responsibilities associated with providing superior services and care to our patients, we hope that protecting their privacy is something easy to do. Our policies and our program are meant to make it easy for employees to understand their obligations under our privacy policies and to comply and protect PHI. The above tips should help you both avoid a privacy violation and protect the valuable information our patients entrust to us.

UNC Health Care Privacy Audits: *What is the Patient's Medical Record?*

When conducting investigations into potentially unauthorized access to a patient's medical record in Epic, we sometimes hear that the user did not access the patient's chart. In some cases, the user accessed appointments, billing information, or demographic information that resides outside of the **Chart Review** section in Epic.

However, it should be noted that all information in Epic is part of the patient's medical record. This includes, but is not limited to: appointments, demographics, coverage, guarantor information, and reports that contain patient information. The UNC Health Care System (UNCHCS) policy, [Electronic Patient Information Access and Auditing of Access](#), covers all "information that includes PHI and is maintained, collected, used or disseminated by or for UNCHCS."

For the purpose of auditing user access, no distinction is made with regard to whether the access was to a patient's chart (**Chart Review**) or limited to other areas of the medical record. Sensitive and confidential information resides in many areas of the Electronic Health Record (EHR) and all access should be limited to a **Business Need to Know**.

The **PRIVACY OFFICE**

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

Phone: 984-974-1069

Hotline: 1-800-362-2921;
hotline.unchealthcare.org

Privacy@unchealth.unc.edu



Regulatory Lunch & Learn Series

Need more Compliance information? Please email compliance@unchealth.unc.edu to receive an invitation to the monthly Lunch & Learn regulatory update WebEx, held the third Monday of the month.



Word Scramble: 18 HIPAA Identifiers

The HIPAA Privacy Rule requires us to protect individually identifiable health information. Complete the Word Scramble below to show the 18 HIPAA Identifiers:

1. ENAM _____
2. DREADSS _____
3. AETDS _____
4. HOENP RUMBEN _____
5. AFX ENMBRU _____
6. IMLAE DEDASRS _____
7. LCIOAS RTYUCSIE BENRUM _____
8. LCMEDAI OREDCR MNRUBE _____
9. ATLHEH ALPN FANEEYIBRCI # _____
10. CUNACTO NUSBEMR _____
11. FTECCIETARI / LCNSEIE REMBNU _____
12. HCILEEV NERIFDETII _____
13. EICEDV IIRFEDINET _____
14. BEW LRU _____
15. PI REDSDAS _____
16. IRECMOBIT FETRIEIDIN _____
17. OGTAIRCHPOPH GEIMSA _____
18. ROTHE EIQNUU REEITDFNI _____

Answers
 1. NAME 2. ADDRESS 3. DATES 4. PHONE NUMBER 5. FAX NUMBER 6. EMAIL ADDRESS
 7. SOCIAL SECURITY NUMBER 8. MEDICAL RECORD NUMBER 9. HEALTH PLAN BENEFITARY # 10. ACCOUNT NUMBERS 11. CERTIFICATE / LICENSE NUMBER 12. VEHICLE IDENTIFIER 13. DEVICE IDENTIFIER 14. WEB URL 15. IP ADDRESS 16. BIOMETRIC IDENTIFIER 17. PHOTOGRAPHIC IMAGES 18. OTHER UNIQUE IDENTIFIER