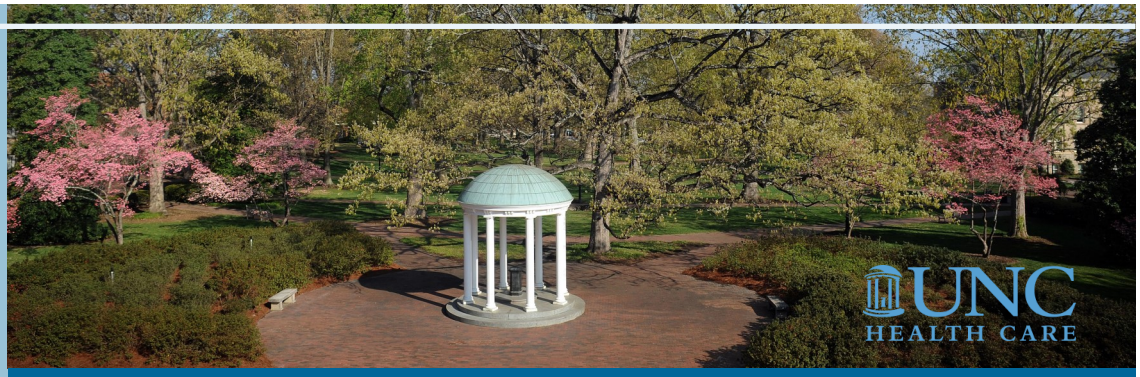
The PRIVACY QUARTERLY



Volume 4, Issue 1 July 2018

Timely Privacy Incident Reporting

As UNC Health Care System employees, we are all responsible for protecting patient health information. Privacy incidents involving patient data affects our ability to improve the health of all North Carolinians and provide high-level, quality care. Incidents involving the unauthorized access, use, or disclosure of patient information can cause distrust and negatively impact a patient's relationship with UNCHCS.

While we, as a community, try our best to avoid privacy incidents through vigilance and training, we understand that incidents do happen. It is vital that the UNCHCS Privacy Office be notified as soon as possible so prompt action can be taken and further harm to the patient can be prevented. Furthermore, the Privacy Office has only 60 days to investigate the root cause of the incident, mitigate any harm to the patient, initiate staff remediation, and notify the affected individual and government agencies (when necessary). If you are aware of or suspect **any** inappropriate use or disclosure of PHI, please report the incident to the UNCHCS Privacy Office.

To report a known or suspected violation of patient privacy, please contact the UNCHCS Privacy Office through the Online Reporting System (http://hotline.unchealthcare.org/) or call the Hotline at 1-800-362-2921. A member of our team will review your concerns and take appropriate internal action. You may choose to leave your contact information or report the incident anonymously.

Examples of incidents that should be reported:

- Finding documents containing confidential information that were left or discarded or not disposed of in an approved container;
- Unattended computers that have not been locked or logged off, allowing confidential information to be viewed;
- Theft or loss of UNCHCS-owned or personal equipment containing protected health information (PHI);
- Knowledge that a workforce member has accessed electronic medical records out of curiosity or without a legitimate work-related purpose (i.e., accessing the record of a family member, friend, or well-known community member);
- Documents that were faxed to the wrong number;
- Emails containing patient information that were sent to the wrong address or not sent securely when being sent externally;
- Patient reports that they received another patient's information;
- Seeing a social media (i.e., Twitter, Snapchat, or Facebook) post that contains a UNCHCS patient's name or other patient information; and
- Knowledge that a workforce member is using another person's login and/or password for accessing electronic information.

Inside this issue:

Privacy Incident Reporting

1-800-362-2921

hotline.unchealthcare.org

Privacy Guidance

984-974-1069

Privacy@unchealth.unc.edu

UNC Health Care: Accessing Family and Friends' Medical Records

With more than 40,000 individuals that have access to the UNCHCS electronic health record system (Epic), which contains extensive medical records on hundreds of thousands of patients, it is critical that UNCHCS employees understand when it is appropriate to access records in Epic. UNCHCS policy requires that there must be a business reason behind each and every access into a patient's medical record. This means that when a UNCHCS employee is in Epic pulling up patient records, the access should be for a business reason.

UNC MC and Rex employees were formerly permitted to access their own medical records or records of others (such as friends and family—if they signed an authorization) directly in Epic pursuant to UNC MC and Rex policy. **Those policies have been retired and employees may no longer access their own medical records or records of their friends and family in Epic.**

Currently, UNCHCS employees are only permitted to use and access Epic for "business" purposes related to their job. Accessing one's own medical records or the records of friends or family in Epic is not an appropriate "business" reason to be in Epic.

Is there a business-need-to-know reason supporting your access of patient records in Epic?

These are examples of accesses that may not be for a business purpose:

- Family, Friends, or Neighbor;
- Co-worker; and
- High-Profile Patient—such as a celebrity, athlete, or public figure.

Our new state-of-the-art Epic auditing application provides continuous automated monitoring of all accesses into Epic. Any access of patient records in Epic made by employees for non-business purposes is flagged by the auditing application and a detailed report is sent to the UNCHCS Privacy Office for investigation.

Here is a summary of the process we follow when a UNCHCS employee accesses a patient account without a business reason:

What Happens when the Privacy Office Discovers that a UNCHCS Employee has Inappropriately Accessed a Patient's Account?

Interview Employee's Supervisor	Meet with Employee	Determine Appropriate Level of Discipline	Discuss with Employee's Supervisor and HR	Document Discipline & Notify Patient and Fed. Gov't
Share results of initial audit with supervisor. Seek guidance on whether access was for a defined business reason.	Discuss results of audit with employee to determine if access was for a defined business reason.	Review UNCHCS Privacy Office Discipline Matrix – and determine discipline level for the violation.	Determine appropriate discipline.	Document incident in Privacy Office incident management system. Send written breach notification to the patient (which may identify you by name) and to the HHS Office for Civil Rights.
If no legitimate business purpose is identified – move to next step.	If no legitimate business purpose is identified – move to next step/discipline.			

So, what should you do when you want to access the patient records of your family members, friends, or co-workers—when these people want you to see their records? The solution is for the friend or family member to set up a MyUNCChart account. Patients are now able to create their own account online that permits them to access their UNCHCS medical records at https://myuncchart.org/mychart/. MyUNCChart allows patients to view their own medical records and test results from services provided at UNCHCS facilities as well as other facilities who share their medical records with UNCHCS. Patients can also request in their MyUNCChart account copies of records that may not otherwise be available through MyUNCChart. Additionally, patients can set up a "proxy" access where another individual of their choosing is issued access credentials and is permitted to access that patient's medical records.

For family members or friends who would like a UNCHCS employee to access their records, the family member or friend should set up their own MyUNCChart and then follow the instructions for setting up proxy access allowing the UNCHCS employee to access that patient's records in MyUNCChart. Employees who are patients should also use MyUNCChart to access their own records.

UNC Health Care: FY 2018 Privacy Program Look-Back

At the end of each fiscal year the UNCHCS Privacy Office takes a look back over the last twelve months of work effort to identify issue trends which help us set our goals for the year ahead. Based on this review we see that the UNCHCS workforce is keeping patient privacy top of mind by reaching out to ask for consultations and reporting privacy concerns. We are available to assist you with any of your privacy-related needs and hope that you will contact us in FY 2019 if you have any questions or see anything that raises concerns.

The UNCHCS Privacy Office is available for consultation by calling our main number (984-974-1069) or contacting individual team members. Some common consultations we receive include:

- Requests for assistance with releasing PHI;
  - ◊ Unique circumstances can complicate this decision and we are here to help you when needed.
- Requests for a member of the Privacy Office to participate in discussions surrounding a new process or policy that is being established in a treatment or operational location/department;
  - ◊ Keeping Privacy in mind from the beginning of a new process minimizes the potential for privacy violations once it is implemented.
- UNCHCS Privacy Policy questions; and
  - ◊ We are glad to help you locate or interpret a privacy policy anytime.
- Patient's Rights.
  - ◊ Patients have specific rights under HIPAA and each employee should know how to help a patient exercise those rights. If you are unsure, we are here to help.

The Privacy Office saw a 17% increase in the number of investigations that were conducted across UNCHCS owned entities in FY 2018. While a majority of our incidents (65%) are substantiated, many are minor issues that do not result in corrective action for employees. It is important that we are made aware of all issues because UNCHCS has a responsibility to assess each breach of PHI to determine if more than a low probability of compromise has occurred and notify the patient, when required. Concerns that should be referred to our office for investigation include:

- Misdirected documents, faxes, or emails that contain PHI;
  - ◊ After visit summaries, discharge documents, faxes, or emails that are sent to the wrong person should all be reported to our office for assessment.
- Patient expresses concern that an unauthorized party has gained access to their medical information;
  - ◊ A member of our team will determine if any inappropriate access has occurred and will work with management and human resources to address any substantiated violations.

Continued on page 4

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

https://unchcs.intranet.unchealthcare.org/dept/ACP/privacy/

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.

Continued from page 3

- Vendors, or Business Associates, who have access to our patient information report that they have experienced a breach of patient information;
  - ◊ These should be referred to our office so that we may work with the vendor to ensure an appropriate response.
- ·Patient information released on social media; and
  - ◊ Please provide a screen shot of the information that has been posted to assist us in the investigation.
- Stolen or lost devices that contain patient information.
  - ◊ This should be reported to ISD first and our office will work with them if they determine that patient information has been compromised.

And, finally, our office has provided more training sessions in FY 2018 than ever before. Privacy policies are reviewed at each New Employee Orientation to ensure that new members of our workforce understand the importance of patient privacy. The UNCHCS Privacy team is available to attend your department's staff meeting to discuss any privacy-related topics that would benefit your location. Please contact us to discuss how we can help your department remain compliant with our patient privacy policies. The Privacy Office can be reached by email (privacy@unchealth.unc.edu) or by phone (984-974-1069).

UNC Health Care: Privacy Tips

Spotlight on Emailing PHI

Email is an acceptable method to send protected health information (PHI) if done securely. In order to be compliant with HIPAA and health care system policies, emails containing PHI sent to anyone outside of the UNC Health Care System (UNCHCS) must be encrypted by typing **(secure)** in the subject. This will ensure that the transmission of the email is secure; however, it is important to also be certain that the email address of the recipient is correct. An unencrypted email sent outside of UNCHCS or encrypted emails sent to the wrong person represent violations that should be reported to the UNCHCS Privacy Office.

In addition, PHI entered into the subject is not secure, even when using encryption to protect the transmission of the email. For this reason, we recommend that PHI not be included in the subject of any email, whether sent within or outside of UNCHCS. Including PHI in the subject line increases the risk of disclosure to an unintended recipient.

Finally, when sending email with attachments that contain PHI, if the message is sent outside of UNCHCS the attachment must be encrypted separately from the email. Passwords to encrypted file attachments should always be sent in a separate email. If an email with an attachment that contains PHI is sent within UNCHCS, the attachment needs to be encrypted if it contains PHI of 500 or more people. Again, when encrypting the attachment, you must send the password in a separate email.

Please reference the links below for policy guidance and tips to help you decide what may be sent by email and how to securely send PHI through email.

- https://unchealthcare-uncmc.policystat.com/policy/4728507/latest/
- https://collab.unchealthcare.org/sites/InfoSec/SitePages/Email%20Security.aspx.