The
PRIVACY
QUARTERLY

Volume 2, Issue 3 January 2017

Special points of interest:

- Tips to Protect Sensitive PHI
- Why Timely Reporting of Privacy Incidents Matters
- Reporting Privacy Incidents
- Privacy Tips

Inside this issue:

Protecting Sensitive Protected Health Information (PHI)

UNC Health Care (UNC HC) HIPAA policies require all employees to protect the privacy of PHI. PHI is health information, including demographic data, created or received by UNC HC entities which relates to the past, present, or future physical or mental health or condition of an individual; the provisions of health care to an individual; or the past, present, or future payment for the provisions of health care by an individual and that identifies or can be used to identify the individual.

Sensitive PHI includes information related to mental health, drugs and alcohol, HIV/AIDS, communicable diseases, or genetic testing information. Sensitive PHI is distinct from other forms of PHI because of the higher degree of risk associated with an unauthorized release of sensitive PHI. An unauthorized disclosure of sensitive PHI could cause a patient significant harm including reputational harm, discrimination, or mental anguish. A breach of sensitive PHI can be devastating to an individual so it is important for UNC HC employees to understand how to best protect sensitive PHI.

Patient Directed Release to Third Parties

One instance where an employee can protect sensitive PHI is when a patient requests a copy of their medical record from a UNC HC facility. When a patient requests a copy of his or her medical record, a patient will sign a written authorization for the release of their medical record. The UNC HC Privacy Authorization for Release of Medical Information form (available in the UNC HC HIPAA Manual on the Intranet) provides patients with the opportunity to specifically authorize the release of sensitive PHI. While a patient is not required to use the UNC HC form (since they can use any HIPAA compliant form), using the UNC HC form permits the patient to specifically decide whether to release their sensitive PHI as part of their medical record. If possible, the UNC HC Privacy Office recommends use of the UNC HC form to help ensure that requests are processed quickly and accurately and to prompt the patient to consider whether they wish to authorize release of sensitive PHI.

Fax

Another way employees can take extra care to protect sensitive PHI is when sending it by fax. If you must fax sensitive PHI, be sure to call the recipient prior to sending it to verify the fax number and to let them know it is going to be faxed. Ask them to call you once they receive it so you know it has been safely sent and received.

Verbal Disclosures

If you are verbally releasing sensitive PHI, you should verify the identity of the individual with whom you are discussing the sensitive PHI. The UNC HC Privacy Office will soon be publishing its Identity Verification Policy (*currently in DRAFT form - coming soon).*

Continued on page 4

UNC Health Care: Privacy Incidents

What is a Privacy Incident?

Privacy incidents occur when there is an acquisition, access, use or disclosure of a patient's protected health information (PHI) that is unauthorized and not permitted by the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule.

What are Your Responsibilities to Report a Suspected Privacy Incident?

When an employee suspects that a privacy incident has occurred, that employee should immediately report that incident as follows:

- **UNC HC** (and UNC Hospitals, UNC Faculty Physicians, and UNC Physicians Network): report the incident to the UNC HC Privacy Office online by utilizing the Privacy Incident Report form found on the Intranet at: http://intranet.unchealthcare.org/intranet/hospitaldepartments/auditcomplianceprivacy/privacy/incident-reports
- **Network Entities**: report the incident to the Privacy Officer at the affiliated Network Entity where the employee works. A list of entity-level Privacy contacts is maintained at: http://intranet.unchealthcare.org/intranet/hospitaldepartments/auditcomplianceprivacy/Network-Entities

The UNC HC Privacy Office and the privacy offices at our affiliated Network Entities investigate hundreds of privacy incidents each year. Privacy offices investigate incidents, work with staff and departments to develop corrective action plans and, when appropriate, coordinate notification communications to affected individuals and appropriate government officials. In the future, the level of corrective action for a confirmed violation may be determined in accordance with a forthcoming UNC HC Privacy Violation Sanctions Matrix policy (currently in draft). Currently however, sanctions are addressed in the ADMIN 0238 Sanctions policy.

What are Your Responsibilities after an Incident is Reported?

After an incident is reported to an appropriate UNC HC or Network Entity privacy representative, here are your responsibilities:

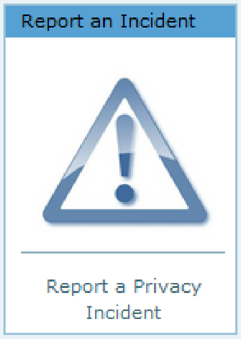
1. **Make yourself available to the Privacy Office for questions.** Inquiries may be conducted via email, telephone, or in person depending on the nature of the incident. Employees and their leaders should be available to answer questions and, in some urgent cases, return to the office or respond to inquiries during off-hours.
2. **Be prepared to provide details about the suspected incident.** The Privacy Office will need to determine the overall risk profile of the incident, including the nature of the PHI and information pertaining to how and to whom the PHI was accessed or disclosed.
3. **Be prepared to take additional actions.**
    - *Disclosures of paper containing protected health information (PHI)*: if a disclosure involves PHI in a paper format (e.g., handing an after visit summary to the wrong patient), the responsible individual and department should make reasonable efforts to reacquire the PHI or request assurance from the recipient that the PHI has been properly destroyed. The most important factor in most incidents is to ensure that the PHI is secured or properly destroyed and not disclosed to any additional parties. Limiting further disclosure or misuse reduces the overall risk associated with the incident.
    - *Electronic Disclosures of PHI:* if a disclosure involves PHI transmitted in electronic format (e.g., an email sent to the wrong recipient), the responsible individual and department should ask the recipient to delete the message from their Inbox or Deleted Items folders and to delete any downloaded attachments. Also, request that the recipient send an email confirming these actions have been completed.

The Privacy Office will seek to determine what type of PHI was disclosed or used, how the PHI was disclosed or used, to whom the PHI was disclosed, and whether the use or disclosure was accidental or intentional. The Privacy Office will also attempt to assess, with the help of department leaders, whether the use or disclosure was solely the fault of the responsible individual or the result of processes and procedures that may need revision.

What Happens after the Investigation is Complete?

When the investigation and breach analysis is complete, the applicable Privacy Office will provide findings to the responsible parties, including recommendations for corrective action or procedural changes as applicable. If it is determined that there is more than a low probability of compromise to the affected patient or patients, the Privacy Office will provide formal notification to the affected individuals and complete the required breach reporting.

Please review relevant policies, including: ADMIN 0139 (Privacy/Confidentiality of Protected Health Information (PHI)) and ADMIN 0239 (PHI Breach Response and Investigation).



To file a Privacy Incident Report, first go to the UNC HC Privacy Office Intranet site and click on the link located under the icon in the top right-hand corner. This will take you to the web page where you can download the fillable PDF Privacy Incident Report form. Complete all fields on the form and save it to your work computer. Then, attach the completed form to a secure email and send it to: Privacy@unchealth.unc.edu. The UNC HC Privacy Office will contact you to discuss the matter and initiate an investigation, as appropriate.

Health System in Illinois Fined $475,000 for Failure to Timely Notify Patients of a HIPAA Breach

Why time is of the essence when reporting a suspected privacy incident to the Privacy Office.

On January 9, 2017, the Office for Civil Rights (OCR) announced a settlement of $475,000 with Presence Health in Illinois as a result of their failure to send HIPAA breach notifications to patients in a timely manner. On October 22, 2013, Presence Health discovered that paper operating room schedules, which contained the protected health information (PHI) of 836 individuals, were missing from the surgery center. Presence Health did not notify patients until February 3, 2014 (104 days after discovery of the incident), even though the regulatory deadline to notify patients is without unreasonable delay and in no case no later than sixty (60) days from the discovery of the incident. The OCR investigation found that Presence Health sent the notification at least forty-four (44) days late and that there were other instances where Presence Health failed to notify patients in a timely manner.

This case is a reminder that time is of the essence when reporting as a suspected privacy incident to privacy offices, such those at UNC Health Care (UNC HC) and its affiliated Network Entities. The UNC HC Privacy Office is responsible for investigating each allegation of inappropriate access, use, or disclosure of patient information. If the UNC HC Privacy Office conducts an investigation and makes a determination that the allegations are substantiated, the UNC HC Privacy Office then determines if the threshold for patient notification is met. To make that determination, the UNC HC Privacy Office conducts a breach analysis using guidance from OCR to consider the type of information that was exposed, the individual to whom it was exposed, any mitigating factors or circumstances and, the disposition of the information.

With all of those factors in mind, if it is determined that more than a low probability of compromise to the information has occurred, then the affected patient(s) and OCR will be notified in writing of the incident. By law, this process — investigation to notification — must take place without unreasonable delay and in no event later than sixty (60) days after the date of the discovery of the incident. It is for this reason that employees are asked to immediately notify the UNC HC Privacy Office when they suspect a breach of patient information may have occurred.

If you are aware of or suspect a breach of patient information has occurred please complete a Privacy Incident Report form at http://intranet.unchealthcare.org/intranet/hospitaldepartments/auditcomplianceprivacy/privacy/incident-reports.

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.

UNC HEALTH CARE

Continued from page 1

Email

If you are sending sensitive PHI via email to an external party, you must encrypt the email transmission. An external email address is any non-UNC email address. An email is secured when the sender types in the Subject field of the email (secure). You should include parentheses when typing (secure) in the Subject field. Entering (secure) first in the Subject field encrypts the sender's email and the recipient will receive a notification that they have received an encrypted email. The UNC HC Information Security Office Email Security webpage provides additional information on how to send secure emails.

Disclosures in the Presence of Family or Friends

Lastly, if a patient is present in the hospital or clinic with another person (i.e., family member, friend, etc.) and the health care provider is considering disclosing sensitive PHI to the patient in front of the other person, the health care provider must first ask the patient if it is okay to speak about their care before discussing the patient's care. To be sure the patient understands what sensitive PHI may be discussed, it is best for the health care provider to ask the visitor to leave and then specifically ask the patient if it is okay for the visitor to return and listen to the conversation. The patient can provide verbal authorization to discuss their care and the patient's agreement to let the visitor listen in can be noted in the patient's chart.

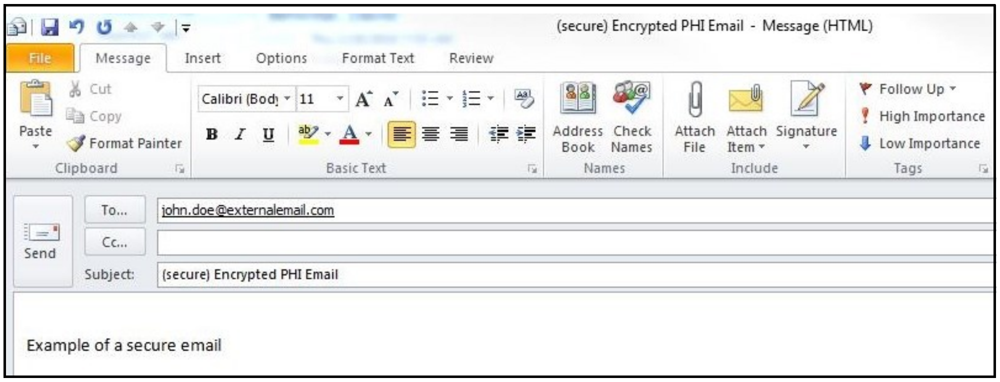
For more information, please consult the Use & Disclosure of Protected Health Information (PHI) Based on Patient Authorization policy (ADMIN 0015) in the HIPAA Manual.

UNC Health Care: Privacy Tips

Spotlight on Secure Email

Below is an example of a secure email.

Make sure to include parenthesis when typing (secure) in the Subject field when sending PHI to an external (non-UNC) email address. Any email attachments that contain Confidential Information must also be password protected before they are sent. For more information, please visit the Information Security Office Email Security webpage.



(secure) Encrypted PHI Email - Message (HTML)

To... john.doe@externalemail.com

Cc...

Subject: (secure) Encrypted PHI Email

Example of a secure email