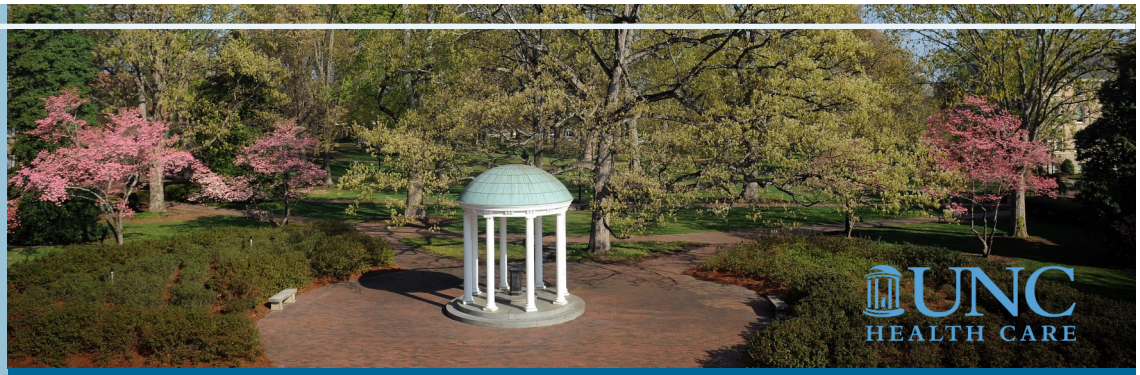
The
PRIVACY
QUARTERLY



Volume 3, Issue 3 May 2018

Special points of interest:

- Prevalence of and tips to avoid insider PHI breaches
- OCR guide teaching you how to get, check, and use your health record
- Importance of conducting a HIPAA risk assessment
- Tips for compliant social media use
- Review of the 15 largest health care security breaches in the last three years

Inside this issue:

Preventing Insider Breaches

Privacy concerns regarding the collection and use of personal information have plagued almost every industry in recent years. It often seems that you cannot turn on the news without hearing about another incident involving misuse or unauthorized release of data. In the last year alone, breaches — like the ones experienced at Humana, Equifax, and most recently Facebook — have affected millions of people and the media has largely focused on external threats to data security. While malware, hacking, and other external factors garner a lot of media attention in the privacy world, health care remains unique in that it is the only industry where internal actors have proven to be the biggest threat to an organization.

In its annual *Protected Health Information Breach Report*, Verizon examined 1,368 incidents involving the mishandling of Protected Health Information (PHI) from 27 countries and discovered that the majority of healthcare-related reportable breaches in 2017 were caused by insiders. Furthermore, simple human error was the root of more than half of those events. Common mistakes included improper disposal of paper documents and errors in the delivery of PHI (e.g., handing discharge instructions to the wrong patient or mistyping a recipient's email address).

Human error is inevitable but we can all help to prevent accidental breaches by remembering to follow these simple tips:

- Always check and double check documents prior to handing them to a patient or another staff member;
- Before sending PHI, in any form, confirm the recipient's contact information;
- Use a cover sheet when faxing PHI;
- Password protect email attachments that contain PHI and secure the email, when necessary;
- Ensure proper destruction of documents containing PHI by placing them in UNC HC approved shredding bins;
- Logoff of or secure your computer prior to walking away from a workstation; and
- Slow down and focus. Many errors occur because we are working too quickly or are distracted.

If you should ever find that you have made an error like this, please self-report it to the UNC HC Privacy Office using our online reporting tool.

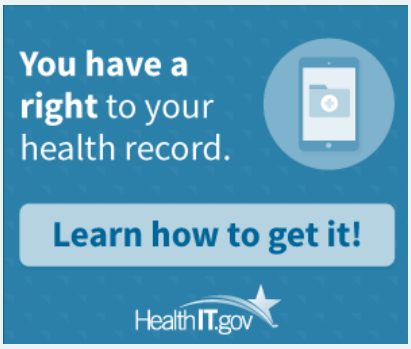
New Guidebook on Health Record Access

The U.S. Department of Health and Human Services' (HHS') Office of the National Coordinator for Health IT (ONC) published a new guidebook to help educate patients about their rights to access their health data, correct mistakes in their record, and use and share their health records. The HIPAA Privacy Rule gives patients the right to obtain copies of their health information held by their providers. Eliminating the obstacles that keep patients from accessing their health information has become a top priority for HHS and ONC and this guidebook is meant to empower patients to access their medical records and actively engage in managing their health.

UNC Health Care (UNC HC) has implemented policies and procedures to ensure that patients have the right to inspect and obtain copies of Protected Health Information (PHI) about themselves. All UNC HC employees should know that patients have this right and should be able to assist the patient in the process. Please direct patients that ask how to gain access to their medical information to Health Information Management (HIM) or utilize the appropriate process at your location. For example, in some outpatient clinics patients can make a request onsite. Patients can choose from several delivery options available to them, including mail, pickup in person, secure email, or fax to another provider. Soon, patients will also be able to request records through their My UNC Chart account.

Please take time to review the information available to our patients on the ONC website and the options available on the UNC HC website for Medical Records and Privacy. Direct any questions about a patient's right to obtain access to their medical information to HIM or the Privacy Office.

For more information, please review the following policies in the HIPAA Manual: Patient's Right to Access, Inspect and/or Obtain a Copy of PHI (ADMIN 0034), Patient's Right to Request Amendments to PHI (ADMIN 0014).



The ONC guide teaches you how to

- Get it — A step by step guide to getting your health record
- Check it — Tips for finding and fixing mistakes in your health record
- Use it — How to use, share, and manage your health record

Fresenius Medical Care Fined $3.5M for Failing to Conduct a Risk Assessment

Fresenius Medical Care North America (FMCNA) recently agreed to pay $3.5 million and enter into a Resolution Agreement with Office for Civil Rights (OCR) to settle allegations that it failed to comply with the HIPAA requirement that the entity conduct a Risk Analysis to identify the risks to the entity's electronic Protected Health Information (ePHI). Headquartered in Germany, FMCNA provides integrated health care to patients who have chronic kidney disease in various facilities including dialysis facilities, outpatient labs, and urgent care centers, etc. In the United States, FMCNA serves over 170,000 patients and has a staff of over 60,000 employees including hospitalists and post-acute providers.

In 2012, FMCNA reported to the OCR that they experienced five separate breaches of ePHI, each at a different Florida location affecting a total of 521 individuals. The breaches each resulted from the loss or theft of devices that were not properly protected through encryption. The PHI compromised in these breaches included names, addresses, phone numbers, dates of birth, treatment dates and details, insurance information, and social security numbers.

OCR initiated a compliance review and found that FMCNA had failed to conduct an accurate and thorough risk analysis and, as a result, impermissibly disclosed ePHI by providing unauthorized access to it for purposes not permitted by the HIPAA Privacy Rule. Additionally, individual facilities failed to implement FMCNA policies and procedures that required them to:

- Safeguard equipment from unauthorized access, tampering, and theft;
- Govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility and the movement within the facility;
- Employ a mechanism to encrypt and decrypt ePHI;
- Address security incidents; and
- Specify the proper functions to be performed, the manner in which those functions were to be performed, and the physical attributes to the surroundings of a specific workstation or class of workstations that can access ePHI.

UNC Health Care (UNC HC) takes seriously the obligation to protect patient information in all forms and has conducted a Risk Assessment to ensure that any vulnerability to patient information has been identified and addressed. Each UNC HC facility is expected to comply with UNC HC Privacy and Information Security Policies regarding the use, transmission, and storage of PHI and ePHI. Should any employee have concerns that their facility may not be compliant with UNC HC Policies they should report it to the UNC HC Privacy Office through the online reporting system. Reporters can always remain anonymous.

Please review relevant policies in the UNC Health Care HIPAA Manual such as: Information Security (ADMIN 0082), PHI Breach Response and Investigation (ADMIN 0239) and Workstation Security (ADMIN 0187).

PHI and Social Media: Compliance Reminders

Recent headlines and Congressional activity have raised questions about the amount and use of data being collected by social media platforms. For example, concerns have been raised that Facebook is collecting data about users' medical conditions without appropriate authorization.

In light of all of this attention concerning social media, it is important that UNC Health Care employees review and be compliant with our Social Media policies. Important reminders and tips include:

- Never post protected health information or confidential information of any kind on social media or blog sites (e.g, Facebook, Twitter, LinkedIn, Pinterest, WordPress, etc.).
- If you see patient information posted on social media by a UNC Health Care coworker, you have an obligation to report it to the Privacy Office.
- If you have questions about social media posts, please contact the UNC Health Care Privacy Office or your local Privacy Officer.

At UNC Medical Center, please review the Social Media Policy (ADMIN 0228). In addition, the annual Privacy, Confidentiality, and Information Security module in Learning Made Simple discusses social media usage.

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.

UNC HEALTH CARE

HIPAA Security Breaches: Recent Trends

Summarizing an article appearing in the March 30, 2018 HIPAA Journal.

Over the last three years, there have been 955 major security breaches in health care that have resulted in the exposure of over 135 million health care records. More than 41% of Americans have had their protected health information (PHI) exposed as a result.

In the last three years, the HHS Office for Civil Rights (OCR) collected more than $49 million in financial penalties from HIPAA enforcement actions.

Of the fifteen largest security breaches in health care in the last three years:

- The covered entity most commonly affected was a health care provider (7/15 breaches), but health care plans (6/15) and business associates (2/15) were also affected and
- The cause of the breach was most commonly a hacking and/or IT incident (13/15 breaches). The remaining breaches were due to either theft of physical records and unencrypted electronic devices with PHI or unauthorized access/ disclosure.

Rank	Year	Covered Entity	Entity Type	Records	Breach Cause
1	2015	Anthem, Inc. Affiliated Covered Entity	Health Plan	78,800,000	Hacking/IT Incident
2	2015	Premera Blue Cross	Health Plan	11,000,000	Hacking/IT Incident
3	2015	Excellus Health Plan	Health Plan	10,000,000	Hacking/IT Incident
4	2015	University of California Los Angeles Health	Health Care Provider	4,500,000	Hacking/IT Incident
5	2015	Medical Informatics Engineering	Business Associate	3,900,000	Hacking/IT Incident
6	2016	Banner Health	Heath Care Provider	3,620,000	Hacking/IT Incident
7	2016	Newkirk Products, Inc.	Business Associate	3,466,120	Hacking/IT Incident
8	2016	21st Century Oncology	Health Care Provider	2,213,597	Hacking/IT Incident
9	2015	CareFirst BCBS	Health Plan	1,100,000	Hacking/IT Incident
10	2016	Valley Anesthesiology Consultants	Heath Care Provider	882,590	Hacking/IT Incident
11	2016	County of Los Angeles Departments of Health and Mental Health	Health Care Provider	749,017	Hacking/IT Incident
12	2017	Commonwealth Health Corporation	Health Care Provider	697,800	Theft
13	2015	VA Dep't of Medical Assistance Services	Health Plan	697,586	Hacking/IT Incident
14	2016	Bon Secours Health System	Health Care provider	651,971	Unauthorized Access/Disclosure
15	2015	GA Dep't of Community Health	Health Plan	557,779	Hacking/IT Incident