The
PRIVACY
QUARTERLY

Volume 4, Issue 2 October 2018

Inside this issue:

Privacy Incident Reporting

1-800-362-2921

hotline.unchealthcare.org

Privacy Guidance

984-974-1069

Privacy@unchealth.unc.edu

Why HIPAA Training Matters

The UNCHCS Privacy Office recently released the 2019 Privacy, Confidentiality and Security annual training e-module in LMS. This module is in addition to other educational resources offered by the Privacy Office, such as new employee orientation training, our set of approximately 50 UNCHCS privacy policies, and SharePoint content on our department website.

HIPAA training is important for various reasons. By completing HIPAA training, you help UNCHCS ensure that the protected health information of our patients is continuously kept confidential and secure. Patients who come to a UNCHCS facility for treatment receive superior care and that is something we can all be proud of. Those same patients also deserve to have their sensitive personal, medical, and financial information in our medical records systems and in our possession protected from unauthorized use or disclosure.

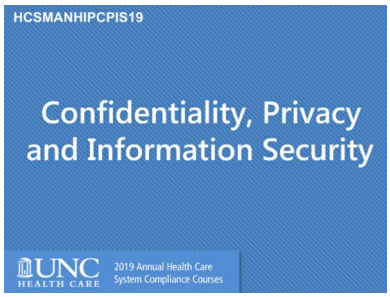
HIPAA training may also reduce privacy incidents by helping employees understand compliant and non-compliant behavior. Last year, there were more than 600 privacy incidents occurring at UNCHCS reported to the Privacy Office, and each year that number continues to rise. More than half of those incidents were deemed to be violations of UNCHCS privacy policies. Many people lose their jobs at UNCHCS each year for committing privacy violations. In the last two years, approximately 25,000 patients were notified in writing by our office of a privacy breach involving their information at UNCHCS. By completing HIPAA training, you learn how to report and reduce the likelihood of privacy incidents.

Lastly, it is important to remember that regulations and the HIPAA Training for UNCHCS Workforce policy require the UNCHCS workforce to complete appropriate HIPAA training.

Thank you in advance for completing your HIPAA training and contributing to a culture of privacy and compliance at UNCHCS.

PolicyStat™

LMS



Protect Patient Information Like You Would Protect Your Own

Nowadays we do so much online. We shop, pay bills, and even bank from the comfort of our own homes. It often seems that the passwords we have created are the only things protecting our private business affairs from exposure. We all know that one slip-up could reveal important identifying information to everyone and that it is important to take steps to secure those passwords and ensure no one else accesses our online accounts.

It is just as important to carry those practices over to work. We deal with sensitive protected health information (PHI) on a daily basis. The devices and applications we use at work hold information about our patients, their medical histories, and their billing/payment information. We need to be just as vigilant in protecting access to our work accounts as we are for our own personal information. Unfortunately, research suggests that credential sharing in health care is extremely common. A 2017 study, by Hassidim *et al.*, found that, out of 299 surveyed medical professionals, 73% had used a coworker's password to obtain access to the electronic health record, thereby increasing the risk of inappropriate use and/or disclosure of PHI.

In addition to increasing risk to the PHI our patients have entrusted us with, credential sharing is against UNCHCS policy. At UNC Medical Center, the Information Security Policy clearly states that employees must "keep personal authentication devices (e.g., passwords, SecureCards, PINs, etc.) confidential." The following best practices will help protect your log-in information:

1. Never share passwords with others or let others watch while you type your password;
2. Never use someone else's password;
3. Do not write your password down or make it easily accessible for others to view;
4. Properly log out of all accounts when stepping away from your computer; and
5. If someone else asks to use your workstation, log out and have them log back in under their own credentials.

For more information, please see the Password Control Standards attachment to the UNC Medical Center Information Security Policy.

HIPAA and Natural Disasters

In the aftermath of a natural disaster, like Hurricane Florence, it is important to understand that the HIPAA Privacy Rule remains in effect. However, in order to help hospitals and providers in affected areas, the Secretary of Health and Human Services (HHS) has the authority to waive some provisions of the Privacy Rule.

On September 11, 2018, the Secretary of HHS did just that when Hurricane Florence hit the United States, thereby providing an exemption from penalties and sanctions under HIPAA. The waiver also permits disclosures to family and friends of a patient and relieves the healthcare entity from having to deliver the notice of privacy practices (NPP) and comply with certain patient requests. These waivers apply only to facilities in an emergency area and for a time period designated by the Secretary. More importantly, regardless of an emergency waiver, HIPAA allows sharing of patient information for treatment and for reasons that are determined in the interest of the patient or public health. During these situations, we must still protect patient privacy, but HIPAA should not impede patient care.

Please click here for more information about HIPAA during Hurricane Florence.

Hackers vs. HIPAA. . . What Is Your Part in the Fight?

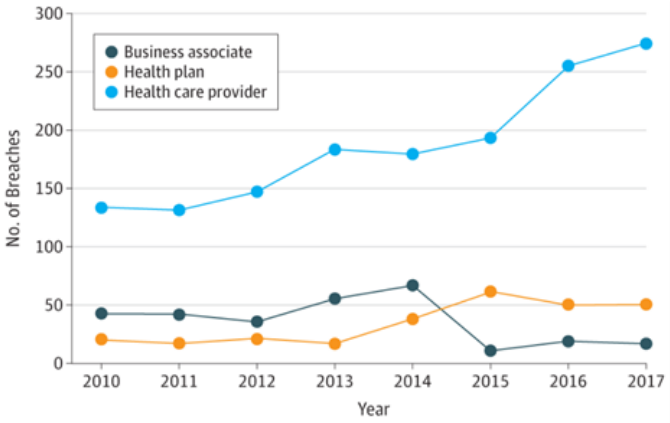
In this Informational age where the modernization of medicine goes hand in hand with the instant gratification of technology, healthcare professionals find themselves not only caring for patients but also for their digital footprints.

Every day we see news stories about breaches of personal and financial information from large box stores to social media giants where millions of people are affected by "hackers" who have acquired personal and financial information on consumers. This risk is no different in health care, where we are tasked as gatekeepers to the electronic medical record (EMR) system as part of our everyday job responsibilities. For each patient encounter, identifiers may range from an address, phone number and social security number, to a checking account, credit card and insurance provider number. If you add those personal identifiers to an individual's diagnosis and treatment information you have a virtual playground for those who may want to use or access this information for their own personal gain.

The American Medical Association (AMA) concluded in a recent study of a seven-year period from 2010 to 2017, that there were 2,149 breaches containing 176.4 million patient records. As seen in the chart below, healthcare provider breaches have not only had the highest frequency, but also the sharpest increase over time in comparison to other measured healthcare-related entities.

The most common entity breached was a healthcare provider, with 1,503 breaches (70%) compromising a total of 37.1 million records (21%). The 278 breaches (13%) of health plans accounted for the largest share of breached records, 110.4 million (63%). Figure 1 illustrates an increasing number of breaches associated with healthcare providers over time.

Data & Chart: McCoy Jr. et al., 2018, "Temporal Trends and Characteristics of Reportable Health Data Breaches, 2010–2017"



Cumulative records breached, millions

Business associate	1.5	10.5	11.6	12.6	21.0	25.0	28.5	28.7
Health plan	3.6	3.7	4.0	4.1	6.2	109.1	110.0	110.4
Health care provider	0.8	5.0	6.3	12.1	14.1	20.5	32.7	37.2

It is the responsibility of the Privacy Office to implement safeguards, policies, and informational resources to support the UNCHCS workforce and strengthen organizational awareness. Please take the time to reference the tools on the Privacy Office SharePoint site (https://unchcs.intranet.unchealthcare.org/dept/ACP/privacy/) and feel free to contact our office with any additional questions you may have.

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

The Way You Use Recycling Bins Can Compromise Patient Information

Blue recycling bins like the one pictured here are widely used across the UNC Health Care System for two different reasons. Some work areas use them as you would expect: to collect aluminum cans and plastic or glass bottles for recycling. Other areas use them to temporarily store documents that contain confidential information, such as protected health information (PHI), until they can be taken to a secure shred bin. The rationale for this second use is that it saves the employee time when they don't have to walk to the secure shred bin each time they must dispose of PHI.

The UNCHCS Disposal/Destruction of PHI policy and UNC Medical Center Hard Copy and Electronic Information Disposal Policy permit this second use of the blue bins in non-public areas only and state that employees who use them for PHI are responsible for emptying them into the secure shred bin every day. The risk associated with this use is present when the employee forgets to empty the bin and a well-meaning member of the environmental services team takes it out with the daily trash. This constitutes a breach of patient information that must be reported to and investigated by the UNCHCS Privacy Office.

The Privacy Office has responded to multiple incidents over the years where an employee's blue bin was emptied in error with the regular trash during the overnight cleaning. This often occurs in locations where a third party is contracted for environmental services and they are not familiar with how we use these bins. They may empty your blue bin without knowing that the information inside requires special handling and secure disposal.

To prevent this from happening in your area, we encourage you to take another look at how and why you use these blue bins. If you determine that it is operationally beneficial to continue to use them for the temporary storage of PHI then please be sure you are managing the associated risk by emptying them into the secure shred bin at the end of each day, as required by the UNC Medical Center Hard Copy and Electronic Information Disposal Policy.

If you find that your bin has been emptied with the regular trash, please notify your supervisor and file a report with the UNCHCS Privacy Office at http://hotline.unchealthcare.org right away. For more information about the appropriate disposal of PHI, please review relevant policies or contact the UNCHCS Privacy Office at 984-974-1069 or privacy@unchealth.unc.edu.

UNC HC: HIPAA Policy Manual

Please remember that UNCHCS HIPAA Policies are now accessible from the Privacy Office website at: https://unchcs.intranet.unchealthcare.org/dept/ACP/privacy/Pages/unchcs-policies.aspx.