



**Inside this issue:**

Texting and Emailing PHI	2
HIPAA Right of Access	2
UNC Health: Discontinue Use of Spanish NPP Poster	3
Word Search: HIPAA Terminology	4

**Privacy Incident  
Reporting**

1-800-362-2921

hotline.unchealthcare.org

**Privacy Guidance**

984-974-1069

Privacy@unchealth.unc.edu

## Healthcare Breaches have become Daily News

Healthcare data breaches have become daily news. That's largely because stealing healthcare records is a lucrative business. Healthcare records can contain personal, medical, and financial information that a criminal can use for identity theft. Healthcare regulations offer a thorough set of regulatory protections against breaches. However, despite all of the regulatory requirements to prevent data breaches, they are still all too common across the industry. Numerous hospitals and physician practices across the country and the world have been crippled by phishing attacks and ransomware. Payouts in Bitcoin and other cryptocurrencies to overseas hackers are the only way out for some healthcare institutions that succumb to a ransomware attack.

Here are two ways we can protect our protected health information and our Health Care System from suffering a substantial privacy data breach. The first is to be ever vigilant regarding email. Many hackers find their way into an organization through a phishing email. The stakes are much higher now that phishing emails look increasingly like legitimate internal business emails from someone you may trust in the organization. All too often, the phishing email manages to fool the recipient and trick that individual into entering their network user name and password into a bogus website. This simple mistake can lead to catastrophic consequences, subjecting untold numbers of patient records to a potential privacy breach. Remember, nobody internal to our organization should ever ask you to disclose your user name and password in an email.

The second method we can all utilize to better protect our data is to ensure that the data we send, receive, and store in emails is minimized to the extent practical and is at all times secure and encrypted when appropriate.

Our UNC Health Information Security Department offers many resources and educational materials on securing emails and securing data in emails — whether that data is in attached documents or in the body of the email. Here are links to those resources:

- [Protecting Data](#)
- [Emailing Securely](#)
- [Encrypting Microsoft and Adobe Files](#)
- [Securing Unstructured Data](#)

Remember, one simple error in judgement could result in potentially catastrophic consequences for our organization. So, please always be mindful of your actions when it comes to email. It is all too easy to gain a false sense of confidence that nothing could go wrong when in fact that is exactly what the criminals are relying upon when searching for their next phishing victims.

## Texting and Emailing PHI ... It's Faster and Easier but Must be (SECURE)!



With technology capabilities moving at the speed of light and access with one click of a button, it is easy to overlook policies and safeguards that govern the protected health information (PHI) we use and disclose daily as healthcare professionals.

As the ONE UNC Health system expands, there are more “players” in the game who must provide the highest level of care to our patients. It is important to remember that although these “players” are part of the same treatment team, they may not be on the same secure network. Even with the allowance of EXTERNAL email addresses in our Outlook system, we must remember that if the email destination is not unhealth.unc.edu it is not internal, and therefore not secure. Emailing PHI to external addresses is permitted, BUT the attached file and the email itself must both be safeguarded though ENCRYPTION. Texting PHI is necessary in certain cases and may be permitted if it adheres to the privacy guidelines provided below. Protecting the privacy of our patients’ PHI is everyone’s responsibility as part of the ONE UNC Health team.

*Emailing PHI to external addresses is permitted, BUT the attached file and the email itself must both be safeguarded though ENCRYPTION.*

*Texting PHI is necessary in certain cases and may be permitted if it adheres to our privacy guidelines.*

If you choose to use email or texting to transmit PHI, you must adhere to our [privacy guidelines](#) in order to keep your patients’ health information secure. Additionally, please utilize guidance from our Information Security Department concerning [Email Security](#) and [File Encryption](#). Using these resources will help you comply with the expectations of our healthcare system and protect our patients’ health information.

---

## OCR Continues to Emphasize the HIPAA Right of Access



On December 12, 2019, the Office for Civil Rights (OCR) announced a second [enforcement action](#) and settlement related to its HIPAA Right of Access Initiative. The Right of Access Initiative is an effort to ensure that patients have prompt access to their medical records in the format of their choice and at a reasonable price. Korunda Medical, LLC (Korunda), a Florida-based provider of comprehensive primary care and interventional pain management was found to have failed to provide medical records to a third party at a reasonable fee allowed under HIPAA. Even after receiving a letter of technical assistance from OCR, Korunda failed to provide the medical records following repeated requests.

As a result of non-compliance with the HIPAA Right of Access, Korunda has entered into a monetary settlement and corrective action plan that includes one year of monitoring by OCR.

As OCR continues to emphasize the HIPAA Right of Access, it is important to comply with patient requests for access to their medical record, including patient-directed requests to third parties. At UNC Medical Center, please direct patients to the [Medical Records and Privacy internet site](#) or advise them to call Health Information Management (984-974-3226) with questions and to request the forms needed to make a medical records request.

If you have any questions about the HIPAA Right to Access, please contact your Health Information Management office or the UNC Health Privacy Office ([privacy@unhealth.unc.edu](mailto:privacy@unhealth.unc.edu) or 984-974-1069).

## UNC Health: Discontinue Use of the Spanish NPP Poster

In summer 2019, the UNC Health Privacy Office issued a new Notice of Privacy Practices (NPP). Many people noticed that we did not re-issue the poster in Spanish and have asked why. The law that requires us to display the NPP in a prominent place at each intake location does not go so far to say that it must also be posted in Spanish. So, simply put, have decided not to display the Spanish NPP poster any longer since we are not required to do so.

### But what about our Spanish-speaking patients?

The Privacy Office wants to ensure that all patients have access to the NPP. Because Spanish is the most common non-English language spoken by our patients, the NPP has been produced in Spanish and is available in a brochure and electronic format in that language. Clinics with a high Spanish-speaking patient population are encouraged to order the Spanish NPP Brochure to have on-hand for any patient that may ask for it.

For more information about how to order the brochure in English or Spanish, visit the [Notice of Privacy Practices](#) page on the Privacy Intranet. If a patient asks you for a Spanish version of the NPP and you do not have a Spanish NPP Brochure on hand, it can be printed on demand from [this internet location](#).

### What should I do with the old Spanish NPP that we have in our location?

Please remove any old versions of the Spanish NPP Poster that you may have on site. They should not be displayed any longer as they do not reflect the most recent changes. Only the most up-to-date version should be offered to patients.

If you have any questions about the Notice of Privacy Practices, please contact the UNC Health Privacy Office at 984-974-1069.

The NPP is Available in Three Formats for Different Purposes		
Poster 	Brochure 	Electronic 
<p>The law requires that all intake locations at each UNC Health facility post an English NPP in a conspicuous place on the wall. We have interpreted that to mean that all registration locations must display an NPP Poster on the wall of their location.</p> <p>The poster must be mounted in a frame where patients can read it.</p> <p>It is not necessary to display the NPP Poster in Spanish, but locations must provide a printed NPP in Spanish if it is requested. As needed, please provide the Spanish NPP in brochure format or download and print an electronic copy.</p>	<p>Patients who request a copy of the NPP are often given a brochure. These are available in English and in Spanish.</p> <p>It is not required that each patient be given an NPP brochure and each clinic decides if they will keep these on-hand based on their front desk processes.</p>	<p>The NPP is always available at the bottom of each outward-facing (Internet) UNC Health facility website.</p> <p>Some locations download this e-copy of the NPP in order to print and provide the NPP to patients who ask for it.</p>

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](mailto:compliance@unchealth.unc.edu) to receive an invitation to the monthly Lunch & Learn regulatory update WebEx, held the third Monday of the month.



**Word Search: HIPAA Terminology**

Q L O M D K D Z Y D B W U C W E N R T T V G H A  
 O X U I I N W R B E T R E A T M E N T D G Y M S  
 J T G N S H H D O S A G S I H J B V H D U O I X  
 C N S C C V V S R C V F E D E R A L L A W Z N S  
 I O Y I L M Y P Y X E O D P B X J C H N R N I N  
 E I T D O L I Z A O T R H F H A I I S U U Y M S  
 I T I E S N Z H Y L T S L S I U U O T F K T U E  
 B P L N U E Y X Q O V G W A S G J S W C D I M R  
 Z Y A T R I W Y Y T P A N E C F T I D U A R N U  
 U R I A E I A N V D O S U L F I H P E S W U E D  
 I C T L B X V M M T T T G T K B D K T S B C C E  
 J N N C H G I Y R E D D F S H H H E V Y Q E E C  
 X E E F Y T I T N E D E R E V O C Y M J K S S O  
 G Z D A H B S R G X B A B N I Z R S F D E W S R  
 N D I X M D A N R B R N R J K S Q I B D W D A P  
 I Z F E K I H E I B E S D Q X L S B Z L W S R F  
 R S N X X U L Y Y J A G F I D I N I E A A H Y T  
 O T O F L E T O Z S C H S E I C I L O P T M N H  
 T F C U A O X G A X H H S P X M W Z A X M I J Y  
 I O X S L D V U S S T O R O W P B J J C A S O C  
 N H E P E R F X X H W H U C A C X A H S X Y U N  
 O N O T I F I C A T I O N D O C L J C K B V H V  
 M V Y Y N P F R E C I F F O Y C A V I R P E U O  
 S E C I T C A R P Y C A V I R P D Z S I H M Z Z

- |                   |                |                 |
|-------------------|----------------|-----------------|
| AUDIT             | AUTHORIZATION  | BREACH          |
| CONFIDENTIALITY   | COVERED ENTITY | DHHS            |
| DISCLOSURE        | ENCRYPTION     | EPHI            |
| FEDERAL LAW       | INCIDENTAL     | MEDICAL RECORD  |
| MINIMUM NECESSARY | MONITORING     | NOTIFICATION    |
| OCR               | POLICIES       | PRIVACY OFFICER |
| PRIVACY PRACTICES | PROCEDURES     | RELEASE         |
| SECURITY          | TREATMENT      | USE             |