The PRIVACY QUARTERLY

Volume IV, Issue 4 May 2019

Inside this issue:

Privacy Incident Reporting

1-800-362-2921

hotline.unchealthcare.org

Privacy Guidance

984-974-1069

Privacy@unchealth.unc.edu

New Notice of Privacy Practices (NPP) Coming to UNCHCS

The UNC Health Care Privacy Office is happy to announce that a new Notice of Privacy Practices (NPP) will soon be distributed throughout the System. The NPP is one of the most important documents in the UNCHCS Privacy Program. This document informs patients of their rights under HIPAA and educates them on how we use their protected health information (PHI). The NPP has been revised to update language regarding research, emails, text messages, and participation in the health information exchange. These edits have produced a shorter NPP which has resulted in a poster with a larger font size that is easier for patients to read.

Whenever changes are made to the NPP, patients must have an opportunity to obtain an updated copy. For that reason, the new Version 7 NPP will be available in poster, brochure, and electronic formats to ensure that it is accessible to our patients as soon as possible. Depending on your location, you may use all three of these formats:

1

Poster

The NPP poster **must** be displayed at each patient intake location. This means all UNCHCS clinics and each patient registration area of our hospitals must post the NPP poster in a conspicuous location. The Version 7 poster is the same size as Version 6 so locations that already have a framed NPP will not need to purchase a new frame; simply replace Version 6 with Version 7. Locations that do not have an existing frame may order one from Staples. The poster must be posted in English; it may, but is not required, to be posted in Spanish. Additional instructions to be provided in upcoming communications.

2

Brochure

Previously, clinics kept paper copies of the NPP brochure available for distribution to patients. This is still done in some clinical areas, but is not required. Many clinics use a signature pad to capture the patient's signature on the NPP Acknowledgement Form and offer the patient a copy of the NPP. If the patient accepts that offer or otherwise asks for a copy of the NPP, it must be provided. Clinics and registration areas can decide if they want to keep NPP brochures on hand for these requests or if they want to print an NPP from the electronic location if and when they are asked for one. The brochures will soon be available in both English and Spanish through the UNCH Print Shop.

3

Electronic Version

The NPP must be posted on the external (Internet) website for each of the UNC Health Care System entities. Patients and employees can find the NPP in both English and Spanish in the footer of each entity's Internet website. Additionally, employees will soon be able to view the NPP on the Privacy Office's Intranet page.

Keep watching *News for Employees*, *News for Managers*, and our Intranet page for more information about the new NPP. You may also contact the Privacy Office with any questions you may have by phone (984-974-1069) or by email (Privacy@unchealth.unc.edu).

Northwestern Memorial Reportedly Fired 50 Employees for Snooping: *Why this Matters and How Would this Play Out at UNCHCS*

After *Empire* star Jussie Smollett was seen in the Northwestern Memorial Hospital's ER in Chicago for injuries that later appeared to be the result of a staged attack, dozens of Northwestern Memorial employees reportedly accessed Mr. Smollett's medical records. These employees had no business reason to access his records and were presumably doing so only because they had some personal curiosity about his medical care. The hospital's decision to fire each of the employees who inappropriately accessed this celebrity's records should be applauded. Too often hospitals and health systems claim that they hold in high regard the importance of protecting patient information while failing to actually take meaningful actions in support of their privacy program and protecting patient privacy. Not only do many hospitals fail to take appropriate disciplinary actions for privacy violations involving snooping, but far too many hospitals do too little to proactively identify wrongful access.

At the UNCHCS . . .

We have implemented a state-of-the-art proactive EHR access auditing program that continuously monitors the UNCHCS electronic health record (EHR) for inappropriate accesses. Since its inception more than 15 months ago, we have had hundreds of inappropriate accesses identified with many people losing their jobs as a result of their inappropriate access. We believe that all of our patients — not just celebrities — should have protections in place that identify inappropriate access of their medical records. This is why we have in place our vendor-based program that continuously audits any and all inappropriate accesses that occur within our EHR.

Leadership upholds the Privacy sanctions matrix, which often results in termination of employment for employees who intentionally access an individual's record without a valid business purpose.

We are confident that our program at UNCHCS is sophisticated and mature enough to ensure that, if wrongful access resembling the Jussie Smollet case were to occur here, we would swiftly identify the wrongful access through our EHR access audit program. We are also certain that leadership would support the termination of employment of any employees who wrongfully accessed the records of an individual patient irrespective of whether they were a celebrity or just a regular person like you or me. This has been the case here at UNCHCS and will continue to be the case going forward.

Record Year for HIPAA Penalties

The Office for Civil Rights (OCR) finished 2018 with one civil monetary penalty and ten settlements to resolve HIPAA violations. This was not quite a record for the number of financial penalties, but the total amounts paid — $28,683,400 — is a record. Included in these financial penalties was a $16 million settlement with Anthem Inc., resulting from findings related to a 2015 data breach affecting approximately 78.8 million members. The largest penalty affecting a healthcare provider was a $4,348,000 civil monetary penalty assessed against the University of Texas MD Anderson Cancer Center due to a lack of encryption resulting in the impermissible disclosure of ePHI. According the OCR Director Roger Severino, "Our record year underscores the need for covered entities to be proactive about data security if they want to avoid being on the wrong end of an enforcement action."

All UNCHCS employees should remember that we have a responsibility to protect the privacy and security of protected health information (PHI) and to report any suspected incidents to the appropriate Privacy or Information Security Office.

UNC Health Care: Questions from the Privacy Office Consultation Log

Spotlight on Prospective Employees

The UNCHCS Privacy Office receives hundreds of questions each year from staff members seeking advice as they encounter situations with potential privacy implications. We welcome these questions and encourage discussion with a Privacy team member if employees are navigating a difficult or unique situation. Recently, we received a question that has come up from time to time over the years:

> *We have narrowed the number of candidates for our open position down to three. May we ask them to come into the office and sit with an employee as they work so the candidate can get a sense of what the job would entail?*

While we understand the importance of hiring the right person for the job, inviting someone to participate in any process that includes patients or patient information would likely constitute a privacy violation. Job applicants are not yet members of our workforce and for that reason they cannot be exposed to patients or patient information. However, if at UNCH, you were to register the applicant as a Shadow Visitor through Volunteer Services it may be possible to allow them to observe patient information or patient care areas. The applicant would have to comply with a number of requirements including taking Privacy training, proving that they are current on the immunizations required of staff, and signing a Confidentiality Statement. The sponsoring department accepts responsibility for having these Shadow Visitors on site and must comply with the requirements of applicable Shadow/Visitor policies, which include escorting the applicant at all times. At UNC Medical Center, applicable policies include: Shadowing and Shadow Students or Visitors.

If you have a question for the UNCHCS Privacy Office team, please contact us by phone (984-974-1069) or email (Privacy@unchealth.unc.edu).

Touchstone Medical Imaging Pays $3 Million to OCR and Adopts CAP

Touchstone — a Diagnostic Medical Imaging Services Company headquartered in Franklin, Tennessee — was ordered to pay $3 million to settle a breach which exposed the protected health information (PHI) of over 300,000 patients. In May 2014, Touchstone was notified that one of its web servers allowed open access to its patients' PHI. This server access allowed search engines to index patients' PHI and made PHI viewable on the Internet even after the server was decommissioned. In addition to the monetary settlement, the Office for Civil Rights (OCR) required Touchstone to implement a Corrective Action Plan (CAP) to address major weaknesses in their privacy safeguards for protection of their patients. Components of the corrective action plan included:

- **Business Associates**: evaluate/revise policies and processes used with all vendors to determine if those relationships are eligible for definition as a Business Associate under HIPAA Rules.
- **Risk Analysis/Management**: complete an enterprise-wide, complete analysis of the security risks and vulnerabilities for the organization.
- **Policies and Procedures**: review and revise written policies to bring them into compliance with the privacy, security, and breach notification rules.
- **Training Curriculum**: submit and obtain approval for proposed privacy training materials for employees.
- **Reportable Events Protocol**: establish a process for addressing investigation and reporting of privacy violations by staff members.
- **Annual Reports**: annually submit to OCR a report evaluating Touchstone's progress towards implementing the measures listed in the CAP.

The UNC Health Care System has many policies, procedures, and safeguards in place to avoid an incident like the one above. In addition to reviewing annual privacy training, all employees should familiarize themselves with our Privacy Intranet resources to navigate and protect our patient's privacy.

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

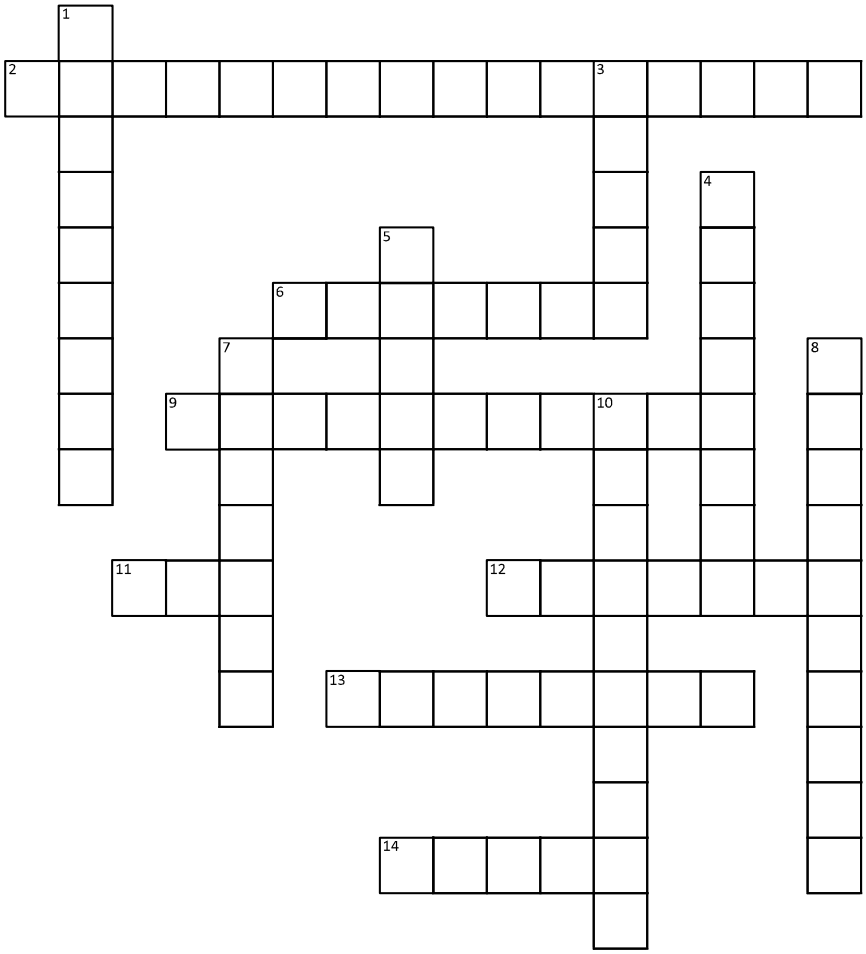
https://
unchcs.intranet.unchealthcare.org
/dept/ACP/privacy/

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

Privacy Crossword Puzzle



Across

2. The _____ (2 words) Policy requires that employees access the least amount of PHI needed to accomplish the task at hand.
6. All patients have the right to_____.
9. Never post patient information or pictures of patients on _____ (2 words).
11. Acronym for Protected Health Information.
12. What do you need to do before sending an email containing PHI to other personal health information?
13. What should you never share with another individual that is used to access systems?
14. HIPAA protects health information in all forms including photographic, electronic, spoken, and _____.

Down

1. A _____ of the patient's privacy occurs when PHI is inappropriately used or disclosed.
3. How many days does the UNCHCS Privacy Office have to investigate a breach and complete notification?
4. What is the minimum frequency for completing the privacy training in LMS?
5. What act was passed to protect individual's medical records and other personal health information (acronym)?
7. Where should you report a suspected breach?
8. What does the e in ePHI stand for?
10. Gossiping about a patient with your friends or family members is an inappropriate _____ of PHI.

Answers: *Across*: 2) Minimum Necessary 6) Privacy 9) Social Media 11) PHI 12) Encrypt 13) Password 14) Paper
Down: 1) Violation 3) Sixty 4) Annually 5) HIPAA 7) Hotline 8) Electronic 10) Disclosure