The
PRIVACY QUARTERLY

Volume 1, Issue 1 April 2016

Special points of interest:

- Contact the UNC Health Care Privacy Office and get Privacy resources
- Federal regulatory developments
- UNC Health Care: Privacy policy updates
- UNC Health Care: Privacy tips and FAQs

Inside this issue:

Welcome!

Jeri Williams
Interim Chief Privacy Officer
Jeri.Williams@unchealth.unc.edu

Sarah Blackmon
Privacy Investigator
Sarah.Blackmon@unchealth.unc.edu

Contact us anytime!

Phone: 984-974-1126
Hotline: 1-800-362-2921

Privacy@unchealth.unc.edu

James T. Hedrick Building
211 Friday Center Drive
Chapel Hill, NC 27517

Welcome to the first edition of *The Privacy Quarterly*, from the UNC Health Care Privacy Office!

This newsletter is designed to improve communication with the UNC Health Care Privacy Office and to provide education on HIPAA Privacy developments and Privacy-related policies at UNC Health Care and the UNC Medical Center (including the Social Media policy, Identify Theft policies, and Privacy policies in the HIPAA and Administrative Manuals).

UNC Health Care — Privacy Office Intranet

On March 31, Audit, Compliance and Privacy Services launched a new website on the UNC Medical Center Intranet.

You may reach the site directly at the link below or by clicking "Depts" on the Intranet@Work homepage. Once there, select "Audit, Compliance and Privacy Services" from the list of hospital departments.

Please visit the new site to review: contact information for UNC Health Care network entities, guidance documents on Privacy issues, physical inspection worksheets, Privacy policies, educational PowerPoints, the Notice of Privacy Practices (NPP), and other resources. You may also use the site to complete an online request for assistance.

http://Intranet.unchealthcare.org/intranet/hospitaldepartments/auditcomplianceprivacy/privacy

Congress: HIPAA Violations at Nursing Homes Involving Social Media

In March 2016, Senator Carper (Delaware) and other members of Congress asked the Office for Civil Rights (OCR) and other regulatory agencies to address potential HIPAA violations at nursing homes. There are concerns that nursing home staff are improperly posting photos of nursing home residents on social media.

According to Senator Carper, a recent investigation by ProPublica identified 37 incidents since 2012 in which workers at nursing home facilities shared on social media photos of residents, some of whom were not fully clothed or were suffering from dementia. In a letter to OCR, Carper noted that many of the individuals involved in the incidents were prosecuted under state laws. However, OCR did not issue public reports as of December 2015 and did not take actions against the nursing homes. Carper asked OCR to detail any enforcement activity involving potential HIPAA violations during the last five years related to social media and nursing homes. Carper also wanted to know whether OCR initiated any compliance reviews of this issue and whether it plans to issue any guidance to nursing facilities about social media use and HIPAA.

On March 15, Senator Grassley (chairman of the Judiciary Committee) asked the Department of Justice (DOJ) to investigate the exploitation of nursing home residents on social media. Two weeks later, the DOJ launched ten Elder Justice Task Forces. Grassley suggested that the photos and social media posts of nursing home residents were meant to degrade and mock nursing home residents for workers' amusement. Grassley noted that much nursing home care is paid through Medicaid and that the nursing home inspection process is a federal-state program. In accepting public money, nursing homes must adhere to state and federal health and safety standards. Senator Grassley also asked the OIG to account for its work on elder abuse, including social media exploitation.

Please *review relevant policies, including: ADMIN 0133 (Recordings of Patients, Staff, and Visitors) and ADMIN 0228 (Social Media).*

OCR: Individual's Right to Access PHI

On January 7, the Office for Civil Rights (OCR) posted guidance aimed at ensuring individuals are able to access their health information in accordance with the HIPAA Privacy Rule.

In a blog post, OCR Director Jocelyn Samuels said "far too often individuals face obstacles to accessing their health information, even from entities required to comply with the HIPAA Privacy Rule." Samuels said the guidance — in the form of a fact sheet and frequently asked questions — is "an important step in clarifying individuals' core right under HIPAA to access and obtain a copy of their health information."

In particular, the guidance addresses the scope of information covered by HIPAA's access right and the limited exceptions to that right, Samuels said.

According to the guidance, the Privacy Rule generally requires covered entities to provide individuals, upon request, with access to information in their medical and other health records maintained by their healthcare providers and health plans.

Individuals do not have a right to access PHI that isn't used to make decisions about them, including quality assessment or improvement records, patient safety activity records, or business planning and management records.

Psychotherapy notes and information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding also are expressly excluded from the right of access.

The guidance also discusses the form and format for providing access to PHI, and emphasizes that covered entities have an "outer limit" of 30 calendar days to respond to a request for access.

The guidance describes the "limited" circumstances when a covered entity may deny a request for access to all or a portion of the PHI requested, including where "a licensed health care professional determines in the exercise of professional judgment that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person."

Please review ADMIN 0034 (Patient Right to Access, Inspect and /or Obtain a Copy of Protected Health Information (PHI).

OCR: HIPAA Phase 2 Audits

On March 21, the Office for Civil Rights (OCR) announced that Phase 2 of the HIPAA Audit Program is set to begin (Phase 2 Audits). OCR is required by the HITECH Act to establish a permanent compliance audit program for HIPAA-covered entities and their business associates. OCR completed the pilot testing for an audit program in 2012 in which it audited 115 covered entities, but it had yet to establish a permanent program.

In its press release, OCR stated that the Phase 2 Audits will focus on desk reviews of HIPAA Privacy, Security, and Breach Notification Rules (HIPAA Rules) policies and procedures, although it also will conduct some on-site reviews.

OCR published an updated audit protocol to assist organizations with conducting their own internal self-audits as part of their HIPAA compliance activities.

OCR has already begun the Phase 2 Audit program by sending covered entities and business associates electronic requests to provide updated contact information. Next, OCR will send pre-audit questionnaires to both covered entities and business associates to determine potential audit pools. OCR emphasized that covered entities and business associates should be aware that electronic communications from OCR are likely, and it is the responsibility of the covered entity and business associate to ensure that any communications are received and not tagged as spam or otherwise filtered.

Desk audits are to be completed by December 2016.

Recent **OCR Settlements**

- $3.9M settlement: laptop stolen with research participants' PHI
- $1.55M settlement: laptop with PHI stolen from business associate
- $25K settlement: physical therapy provider's disclosure of patient information
- $239K settlement against Lincare affirmed

SAMHSA: Proposed Rule on Substance Use Records

On February 9, the Substance Abuse and Mental Health Services Administration (SAMHSA) published a *proposed rule* aimed at facilitating the electronic exchange of substance use disorder information for treatment and other legitimate health care purposes while ensuring appropriate confidentiality protections.

Last revised in 1987, the Confidentiality of Alcohol and Drug Abuse Patient Records regulations, 42 C.F.R. Part 2 (commonly referred to as "Part 2"), need to be modernized to account for the significant changes in the U.S. healthcare system.

The proposed rule, among other things, would require both Part 2 programs and other lawful holders of patient identifying information to have formal policies and procedures addressing security, including sanitization of associated media, for both paper and electronic records.

The proposed rule also would clarify that the prohibition on re-disclosure only applies to information that would identify, directly or indirectly, an individual as having been diagnosed, treated, or referred for treatment for a substance use disorder, and allows other health-related information shared by the Part 2 program to be re-disclosed.

In addition, providers would have more discretion under the proposed rule to disclose records under a "bona fide medical emergency."

The proposal also would permit the disclosure of protected data to qualified personnel for the purpose of conducting scientific research by a Part 2 program or any other individual or entity that is in lawful possession of Part 2 data if the researcher provides documentation of meeting certain requirements related to other existing protections for human research.

Please review relevant policies, including: ADMIN 0021 (Alcohol and Drug Abuse Patient Records) and ADMIN 0011 (Alcohol and Drug Level Determinations).

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.Erb@unchealth.unc.edu to join the weekly *Report on Medicare Compliance* email distribution list and receive PowerPoint updates.

UNC Health Care — Policy Updates

The following Privacy and Security policies were updated between January 1, 2016 and March 31, 2016.

HIPAA Manual (multi-entity)	Administrative Manual (UNC Medical Center)
• ADMIN 0034 — Patient's Right to Access, Inspect and / or Obtain a Copy of PHI • ADMIN 0035 — General Consent for Treatment	• ADMIN 0135 — Police and Investigative Activities in the Hospital • ADMIN 0148 — Release of Patient Information to the News Media • ADMIN 0168 — Shadow Students or Visitors • ADMIN 0202 —Identity Theft Prevention, Red Flag Program • ADMIN 0133 — Recordings of Patients, Staff and Visitors • ADMIN 0228 — Social Media • ADMIN 0019 — Authorized Representatives of Patients • ADMIN 0204 — Disruptive Behavior

In addition, the system-wide UNC Health Care Code of Conduct (System Policy #13) was passed in March 2016. The Code of Conduct reinforces the role and values of the Privacy Office. For instance, the Code of Conduct requires everyone at UNC Health Care to: (1) preserve confidentiality and information security, (2) use social media and

UNC Health Care — Privacy Tips and FAQs

Spotlight on Fax Machines

In your daily job responsibilities, fax is used to communicate with staff, patients, providers, and vendors.

TIP: If you send a fax containing PHI or other confidential information to an incorrect number, report the incident immediately to your supervisor or the Privacy Office.

TIP: Verify fax numbers prior to transmission to ensure the fax will go to the correct person.

TIP: An approved fax cover sheet must be used and must contain a confidentiality notice requesting notification if the fax went to the wrong person.

Policy Reference: ADMIN 0067 (Facsimile Transmission and Receipt of PHI and Other Confidential Information)