The PRIVACY QUARTERLY

UNC HEALTH CARE

Special points of interest:

- Understand the UNC Health Care system approach to Privacy
- Contact UNC Health Care Privacy Officers
- Federal regulatory developments
- UNC Health Care: Privacy policy updates
- UNC Health Care: Privacy tips and FAQs

Welcome David Behinfar, Chief Privacy Officer

Audit, Compliance and Privacy Services is pleased to announce that David Behinfar joined UNC Health Care on July 18 as our new Chief Privacy Officer.

Dave is an attorney who has spent his 20-year career focusing on health care compliance. Dave spent six years in private practice representing clients in a variety of health care transactional and regulatory matters. Over the last 14 years Dave has worked in the privacy offices of the University of Florida, Stanford University, and the University of Wisconsin-Madison. He most recently served as the HIPAA Privacy Officer at UW-Madison and the Senior Director of Privacy at Stanford University.

Dave earned an LL.M. in Health Law from DePaul University School of Law and his J.D. from Southern Methodist University School of Law. He has several professional certifications in health care privacy and security, has published numerous articles, and speaks at national conferences on the topic of health care privacy.

Dave has a son attending the University of Florida and another son in high school. He recently moved to Durham with his 125-pound Alaskan malamute, Luna.

Please join us in welcoming Dave to the team!

Privacy at UNC Health Care — A System Approach

Our mission is to develop a "best in class" Privacy program, providing exceptional service and value to UNC Health Care. "Best in class" means many things, including working as a health care system to collaborate, improve efficiency, and enhance our Privacy processes.

The UNC Health Care Privacy Committee is one means to foster these system-wide efforts. The Committee is comprised of Privacy Officers and other representatives from each UNC Health Care Network Entity and is chaired by the Chief Privacy Officer. The Committee meets monthly to: monitor Privacy trends, develop Privacy best practices, promote standardization of policies and processes (such as those in our HIPAA Manual), foster communication and collaboration, and create a system-wide culture of privacy and confidentiality at UNC Health Care.

Please take a moment to review the list of Privacy Officers (page 3) at our Network Entities and welcome our Chief Privacy Officer:

David Behinfar
Chief Privacy Officer, UNC Health Care
David.Behinfar@unchealth.unc.edu

HIPAA and Mass Casualties: Lessons from Orlando

Following the mass shooting in Orlando, administrators and the public have been wondering whether HIPAA prevents health care facilities from discussing patient cases with the patient's family members and friends. In Orlando, there was such confusion about this issue that Orlando Mayor Buddy Dyer contacted the White House to request a HIPAA "waiver" so doctors could update shooting victims' loved ones about their conditions.

The Department of Health and Human Services (HHS) has since clarified that no waiver was given, nor was a waiver necessary. Unless a patient opts out, hospitals may use a facility directory ("patient list") to inform visitors and callers about a patient's location in the facility and general condition. When, due to emergency or incapacity, the patient has not been provided an opportunity to opt out, directory information may still be made available if doing so is in the patient's best interest (as determined by the professional judgment of the provider) and would not be inconsistent with any known preference previously expressed by the patient.

In addition, providers may discuss the patient's health status, treatment, or payment arrangements with the patient's spouse family members, friends, or other persons identified by a patient where the patient is present (or is otherwise available prior to the disclosure), consents, and has the capacity to make health care decisions. If the patient is not able, due to incapacity or emergency, to provide authorization or object to the use or disclosure, the use or disclosure may still be made if it is in the best interest of the patient (as determined by the provider's professional judgment) and disclosure is limited to PHI that is directly relevant to the person's involvement with the patient's health care. Although consent and authorization should be obtained prior to any disclosure of PHI, emergency care should not be delayed due to the patient's incapacity. If a patient is unable to provide consent before a visit or admission, efforts should still be made, before discharge, to obtain consent or enter a reason why consent could not be obtained following good faith efforts.

Please review relevant policies, including: [ADMIN 0139](#) (Privacy/ Confidentiality of PHI) and [ADMIN 0035](#) (General Consent for Treatment) in the HIPAA Manual.

Filming and Recording Patients

On April 21, 2016, the Office for Civil Rights (OCR) [announced](#) a $2.2 million settlement with New York Presbyterian Hospital (NYP) to resolve allegations that it violated HIPAA by allowing a film crew from the ABC television series "NY Med" to record patients without their authorization at the hospital's facilities. ABC was allowed to film a dying patient and a patient in significant distress without proper authorization. OCR also found that giving the film crews virtually unfettered access to NYP's health care facilities created an environment where PHI could not be protected from impermissible disclosure.

At UNC Medical Center, the ADMIN 0133 policy addresses "recordings" of patients, including films and other images. When patient recordings are made for marketing and public relations purposes by UNC Medical Center representatives, prior authorization must be obtained by the UNC Medical Center News Office and the patient being recorded. Patient authorization is documented in a signed [consent form](#) submitted to the Health Information Management (HIM) department and filed by HIM in the patient's medical record.

When recordings will be performed by members of the external media, ADMIN 0133 requires media representatives to work through the UNC Medical Center News Office to obtain the patient's signed, written consent. The UNC Medical Center News Office will escort external media members and confer with appropriate individuals (e.g., the patient's attending physician) prior to the recording. The policy explicitly states that **"under no circumstances may photographs, films or videotapes be made by media representatives of patients or visitors to a UNCHCS facility if such patients or visitors are unaware, unwilling or reluctant."** Employees should immediately report unescorted photographers or camera crews in patient areas to the UNC Medical Center News Office.

Please review relevant policies, including: the HIPAA Manual policies [ADMIN 0139](#) (Privacy / Confidentiality of PHI) and [ADMIN 0035](#) (General Consent for Treatment) and the UNC Medical Center policy [ADMIN 0133](#) (Recordings of Patients, Staff and Visitors).

Business Associates' Failure to Safeguard PHI

Business associates frequently appear in headlines as sources of HIPAA violations. A "business associate" is a person or entity that performs certain functions, activities, or services for or to a covered entity involving the use and / or disclosure of protected health information (PHI) and is not a component of the covered entity or its work force. Business associates must implement the protections of the HIPAA Security Rule for electronic PHI (e-PHI) they create, receive, maintain or transmit for covered entities; this includes an enterprise-wide risk analysis and corresponding risk management plan.

On June 29, the Office for Civil Rights (OCR) announced a $650,000 settlement with Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS), a business associate providing information technology services to six skilled nursing facilities. 412 individuals were affected by a breach arising from the theft of a CHCS-issued employee iPhone containing e-PHI. OCR found that CHCS failed to safeguard nursing home residents' PHI. At the time of the incident, CHCS had no policies addressing the removal of mobile devices containing PHI from the facility or what to do in the event of a security incident. In addition, CHCS had no risk analysis or risk management plan and the stolen phone had no encryption or password protection.

Please review relevant policies including those in the HIPAA Manual: ADMIN 0022 (HIPAA Business Associate Policy and Procedure), related ADMIN 0022 form (Business Associate Agreement), and ADMIN 0082 (Information Security) policy.

UNC Health Care Network Entity Privacy Officers

Caldwell | Fairy Miller

Fairy.Miller@unchealth.unc.edu

(828) 757-5177

Chatham | Kathy Heilig

Kathryn.Heilig@unchealth.unc.edu

(919) 799-4015

High Point | Kimberly Crews

Kimberly.Crews@unchealth.unc.edu

(336) 878-6000

Johnston | Donna Gibbons

Donna.Gibbons@unchealth.unc.edu

(919) 938-7121

Lenoir |Karl Vanderstouw

kvanderstouw@lenoir.org

(252) 522-7700

Nash | Patricia Cunningham

pscunningham@nhcs.org

(252) 962-8286

Pardee | Andrea Neumeyer

Andrea.Neumeyer@pardeehospital.org

(828) 696-1091

UNC REX | Lisa Walker

(919) 784-3436

Lisa.Walker@unchealth.unc.edu

Wayne | Phyllis Dreading

phyllis.dreading@waynehealth.org

(919) 731-6138

In addition to serving as UNC Health Care Chief Privacy Officer, David Behinfar will serve as the Privacy Officer for UNC Physicians Network, UNC Hospitals, and UNC Faculty Physicians.

UNC Health Care — Policy Updates

The following Privacy and Security policies were updated between April 1, 2016 and June 30, 2016:

HIPAA Manual (multi-entity)	Administrative Manual (UNC Medical Center)
• None updated	• ADMIN 0019 — Authorized Representatives of Patients • ADMIN 0149 — Reporting of Communicable Diseases • ADMIN 0168 — Shadow Students or Visitors

UNC Health Care — Privacy Tips and FAQs

Spotlight on e-PHI

Below are some tips to safeguard electronic protected health information (e-PHI)

TIP: Use "long and strong" passwords that have a creative combination of numbers, letters, and special characters

TIP: Never disclose or share your password and User ID with anyone

TIP: Secure computer systems when you leave your work station

TIP: Turn monitors so that they are not visible to others

TIP: Save e-PHI to a shared drive — not to personal drives

TIP: Only use licensed software

TIP: Report loss or misuse of hospital information to your supervisor, the Privacy Office, IT Security, or Corporate Compliance.

HIPAA Manual Reference: ADMIN 0082 (Information Security); ADMIN 0056 (Hard Copy & Electronic Information Disposal)

UNC Medical Center Policy Reference: ADMIN 0187 (Work Station Security)