The
PRIVACY QUARTERLY

Volume 3, Issue 2 January 2018

Special points of interest:

- Learn about the UNC HC Privacy team
- Review a $2.3M settlement for failing to protect PHI
- Understand OCR HIPAA guidance concerning mental health problems and drug addiction
- Understand reporting timelines under the NC Attorney General's proposals for increased identity theft protection
- Learn how to report Privacy incidents

Inside this issue:

UNC Health Care: Privacy Office Welcomes New Analyst

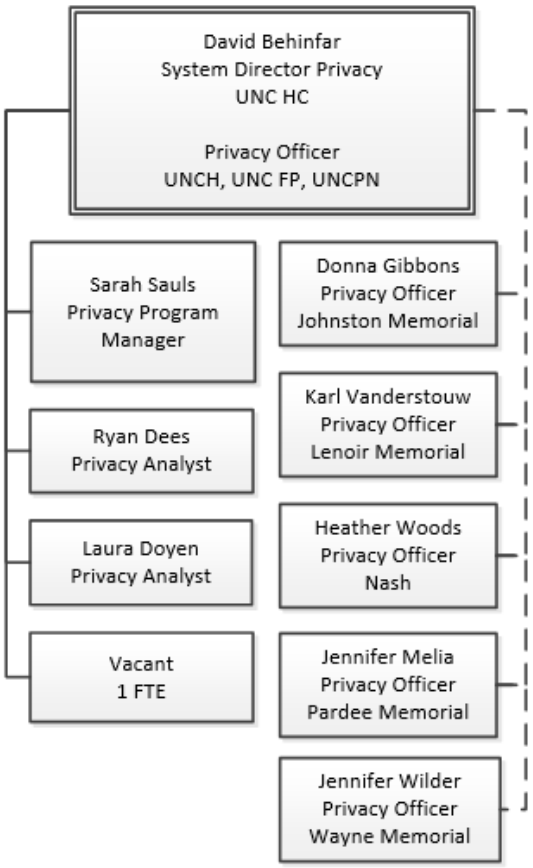
Please join us in welcoming our newest Privacy Analyst to the UNC Health Care Privacy Services team!

Laura Doyen, JD, joined the UNC Health Care Privacy Office in October 2017. Laura comes to us from Chicago where she studied health law and compliance at Loyola University Chicago School of Law. She is also working on a graduate degree in Medical Ethics through the Neiswanger Institute for Bioethics at Loyola's Stritch School of Medicine. While attending school, Laura worked in the Legal Department of Northwest Community Healthcare in Arlington Heights, Illinois and completed an externship with the Renal Legal Team at Baxter International. Prior to moving to Chicago, Laura spent over 15 years coaching gymnastics in Wisconsin.

UNC Health Care: Privacy Office Reorganization

The UNC Health Care Privacy Office is responsible for performing investigations, audits, education, policy development and outreach activities at the UNC School of Medicine (for School of Medicine employees supporting clinical activities) and for and on behalf of entities owned by UNC Health Care (i.e., Caldwell Memorial, Chatham Hospital, High Point Regional Health, Rex Healthcare, UNC Medical Center, UNC Rockingham, and UNC Physicians Network).

Privacy compliance activities arising at entities managed by UNC Health Care may be directed to the Privacy Officer at the relevant entity. Privacy Officers at the managed entities have a collaborative relationship with the UNC Health Care Privacy Office.



21st Century Oncology to Pay $2.3M for Failing to Protect PHI

21st Century Oncology, Inc. (21CO) recently agreed to pay $2.3 million and enter into a Resolution Agreement with the Office for Civil Rights (OCR) to settle allegations that it failed to protect the health records of over 2.2 million people. Based in Fort Myers, Florida, 21CO provides cancer care and radiation oncology services in 17 states and 7 countries in Latin America.

On two separate occasions in 2015, the FBI notified 21CO that its patient information was illegally obtained by an unauthorized third party and offered for sale to an FBI informant. The information available for purchase included patient names, social security numbers, physicians' names, diagnoses, treatment, and insurance information.

The OCR investigation found that 21CO:

- failed to conduct an accurate and thorough risk assessment;
- failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level;
- failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports; and
- disclosed Protected Health Information (PHI) to a third party vendor without obtaining a written Business Associate Agreement (BAA).

UNC Health Care takes the commitment to patient privacy and information security seriously and has implemented proactive Privacy and Information Security Programs to identify and address potential vulnerabilities like these. Employees play a vital role in this program by promptly reporting any concerns they have for patient privacy or information security. Reports can be made online via our online incident reporting tool and employees can either identify themselves or remain anonymous.

Please see relevant policies in the UNC Health Care HIPAA Manual such as: Information Security (ADMIN 0082), HIPAA Business Associate Policy (ADMIN 0022), and PHI Breach Response and Investigation (ADMIN 0239).

OCR Guidance: Appropriate Sharing of Behavioral Health Information with Third Parties under HIPAA

In the midst of a nationwide opioid epidemic, the U.S. Department of Health and Human Services has recognized the role it can play to reduce the harm caused by drug addiction and has issued several guidance documents[1] describing how providers may appropriately share behavioral health information with family members of a patient who may suffer from drug addiction or mental health problems.

"HHS is bringing all of the resources our department has to bear in order to address this crisis. This will ensure families have the right information when trying to help loved ones who are dealing with the scourge of drug addiction," said Acting HHS Secretary Eric D. Hargan.

"We know that support from family members and friends is key to helping people struggling with opioid addiction, but their loved ones can't help if they aren't informed of the problem," said Director Roger Severino, of the HHS Office for Civil Rights. "Our clarifying guidance will give medical professionals increased confidence in their ability to cooperate with friends and family members to help save lives."

The guidance applies to general medical treatment areas[2] and provides several key examples where the provider may inform a patient's loved ones about the medical concerns the provider has with the patient's condition:

1. **Incapacitated or Unconscious Patients**	A provider may share health information with family and close friends who are involved in care of the patient if the provider determines that doing so is in the best interest of an incapacitated or unconscious patient and the information shared is directly related to the family or friend's involvement in the patient's health care or payment of care. For example, a provider may use professional judgment to talk to the parents of someone incapacitated by an opioid overdose about the overdose and related medical information, but generally could not share medical information unrelated to the overdose without permission.
2. **Providers who Seek to Inform Others in Order to Prevent or Lessen a Serious and Imminent Threat to a Patient's Health or Safety**	For example, a doctor whose patient has overdosed on opioids may inform family, friends, or caregivers of the opioid abuse after determining, based on the facts and circumstances, that the patient poses a serious and imminent threat to his or her health through continued opioid abuse upon discharge.
3. **For Notification Purposes**	HIPAA permits health professionals to contact caregivers with information related to a family member, friend, or a person being cared for, that is necessary and relevant to the caregiver's involvement with the patient's health care. For example, if a loved one becomes disoriented, delirious, or is unaware of their surroundings, due, for example, to opioid abuse or a mental health crisis, and arrives at a hospital emergency room for treatment, the doctors, nurses, and social workers may notify the caregiver of the patient's location and general condition.
4. **To Help the Patient**	Doctors, nurses, and social workers may share Protected Health Information (PHI) that is related to the care and assistance being provided by a loved one to the patient. For example, if a caregiver's adult son has been prescribed medication to treat anxiety, and a family member or loved one is helping him by providing supervision or housing, the discharge nurse may inform the family member or loved one what medication he will be taking, if he doesn't object to sharing this information with the caregiver — as well as the side effects to watch for, or symptoms that indicate the medication isn't working or isn't being taken properly.

Helping patients suffering from drug addiction and mental illness stay connected with their family, loved ones and caregivers is a critical component of the multifaceted approach needed to treat individuals with behavioral health conditions.

Should you have any questions about the HHS guidance referred to in this article, please contact the UNC Health Care Privacy Office.

Endnotes

[1] *Guidance includes: How HIPAA Allows Doctors to Respond to the Opioid Crisis and HIPAA Helps Caregiving Connections: HIPAA Helps Mental Health Professional to Prevent Harm.*

[2] *This guidance does not apply to UNC Health Care facilities receiving federal funds in connection with a substance use disorder treatment program (such as at Wakebrook) or any portions of a UNC Health Care facility holding itself out to the public as providing care for drug and alcohol abuse. Please contact the UNC Health Care Privacy Office for further information.*

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

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.

NC Attorney General's Proposal to Strengthen Identity Theft Protection

On January 8, 2018, North Carolina Attorney General Josh Stein and Representative Jason Saine announced proposed legislation to strengthen North Carolina's laws to prevent identity theft and data breaches. The legislation is expected to be proposed in the spring 2018 legislative session.

The legislation includes provisions to prevent breaches, increase consumer protection after a breach, and provide greater control to consumers with regard to the use of their credit report and credit score. Among the proposals is a provision that the entity experiencing the breach must notify the affected consumer and the North Carolina Attorney General's office within 15 days.

If this legislation becomes law, UNC Health Care will need to assess the risk of a security breach and determine whether to notify the consumer and the Attorney General's office within a much shorter timeframe than is currently required. Our current timeframe in which to notify the Attorney General and affected individuals is 60 days.

This radical shortening of the reporting timeframe for applicable breaches will require enormous efforts by the UNC Health Care community to remain vigilant in reporting suspected privacy incidents to the Privacy Office immediately — as well as work diligently to cooperate in any investigation the Privacy Office undertakes to determine whether a breach has in fact occurred.

We will keep you advised of any developments in this proposed legislation.

UNC Health Care: Privacy Tips

Spotlight on Reporting Privacy Incidents

UNC Health Care is committed to a culture where open, honest communication is expected. In 2017, UNC Health Care launched a new Hotline tool that allows for anonymous reporting of Privacy and Compliance concerns. Our policies prohibit retaliation against those who report concerns in good faith.

TIP: Anonymous reports may be made through EthicsPoint for a specific UNC Health Care entity using a new, online incident reporting tool or by calling **1-800-362-2921**.

TIP: Examples of reportable Privacy incidents include but are not limited to: misdirected Protected Health Information (PHI); unauthorized disclosure of, or access, to PHI; inappropriate access to patient information; and potential violations of social media policies.

TIP: The reporter will be assigned a unique code called a "report key" that may be used to check the status of a report for feedback, questions, or to provide additional information.

TIP: All reports are promptly reviewed by the Privacy Office and investigated appropriately.

UNC HEALTH CARE