The

PRIVACY QUARTERLY

Volume IV, Issue 3 January 2019

Inside this issue:

Anthem Pays OCR $16M in Record HIPAA Settlement

The PHI of almost 79 million people was exposed in the largest health data breach in history when Anthem suffered a cyberattack in December 2014. Attackers accessed the Anthem system through spear phishing emails sent to an Anthem subsidiary and at least one employee responded to the email and opened the door to further attacks.

The OCR investigation concluded that between December 2014 and January 2015, the cyber attackers stole the ePHI of almost 79 million individuals including their names, social security numbers, medical ID numbers, addresses, dates of birth, email addresses, and employment information. OCR also determined that Anthem:

- Failed to conduct an enterprise-wide risk analysis;
- Had insufficient procedures to regularly review information system activity;
- Failed to identify and respond to suspected or known security incidents; and
- Failed to implement adequate minimum access controls to prevent the cyber-attackers from accessing sensitive ePHI.

Anthem settled with OCR for $16M and entered into a two-year corrective action plan. In response to this incident, Roger Severino, the Director of the OCR, said, “We know that large health care entities are attractive targets for hackers, which is why they are expected to have strong password policies and to monitor and respond to security incidents in a timely fashion or risk enforcement by the OCR.”

UNCHCS workforce members should always be cautious when opening emails. If you are unsure about something that you received, please contact your local ISD Service Desk to report it. Please review the UNCHCS Information Security SharePoint for more information.

Impermissible Disclosures to the Media

Allergy Associates of Hartford recently entered into an $125,000 settlement with the Office for Civil Rights (OCR) due to a physician’s unauthorized disclosure of protected health information (PHI) to a reporter. The issue began when a patient contacted the local news media to report a dispute with the provider. The physician was then contacted by a reporter and, against the advice of Allergy Associate’s privacy officer, disclosed PHI about the patient. Under most circumstances, the Health Information Portability and Accountability (HIPAA) Privacy Rule requires patient authorization to disclose PHI to a third party. Although the patient initiated contact with the media, the provider was not authorized to disclose the patient’s PHI to the reporter. It is important to remember that the patient’s own disclosure of PHI is not authorization for a provider to respond by disclosing PHI, whether to the news media, on social media, in response to patient reviews, or other unauthorized forums. If you are ever contacted by the news media, please direct the inquiry to your local Marketing or Public Relations Office (at UNC Medical Center: 984-974-1140).

Privacy Incident Reporting

1-800-362-2921

hotline.unchealthcare.org

Privacy Guidance

984-974-1069

Privacy@unchealth.unc.edu

Risks to Patient Information Resulting from Operational Process Change

Most people understand that they are not supposed to access patient information unless it is for a job-related purpose. And it is fairly obvious that when someone loses patient information (like a lost laptop or briefcase containing patient records) that they should contact the Privacy Office. Our office can help provide proactive guidance and consultation to help identify privacy issues up front and help business owners avoid implementing a business practice that by its very nature places data at risk.

Frequent Privacy Violations at UNCHCS

Accessing patient information for non-business purposes

Password Sharing

Posting PHI on Social Media

Accidental Disclosures

Making bad decisions about PHI in Education/ Clinical/ Operations

Mistakes and poor judgment are often to blame for privacy violations. But, a bad business decision involving protected health information (PHI) when establishing a business process in operations can lead to long-term violations extending months and possibly years (until it is discovered) that may place at risk the information of hundreds or even thousands of patients. For example, the decision to allow patients to complete forms with sensitive PHI that are sent to a third party via unencrypted email for a vendor analysis without a business associate agreement (BAA) can pose numerous privacy issues that may go unnoticed for some time.

When business decisions across the health care system are made, considerations such as costs, efficiency, and profitability are most often rightfully addressed. However, privacy compliance should also be part of the decision-making process especially if there is a use or disclosure of PHI that involves a third party outside of UNCHCS. Granted, most arrangements do not require privacy review. But those that do should be identified by business owners who should identify these issues through their own diligence and review. The business owner then has a duty to protect the organization and patient privacy by seeking appropriate advice and guidance.

Last year, our office provided more than 700 substantive privacy compliance consultations on a variety of situations including data sharing and data transfers to third parties, provisioning access to PHI in internal systems (such as Epic) to internal and external personnel, advising on when and if confidentiality and BAAs were required, and many other process and workflow-related projects involving PHI. Our office is capable of providing a comprehensive overview of the privacy considerations in any project or proposed workflow where PHI is being stored, transmitted, used, disclosed, or destroyed. Our involvement in a particular project is usually only temporary and is most beneficial if it is early on in the process; this can have multiple benefits in helping UNCHCS business owners pursue their plans knowing that privacy concerns will not be an issue.

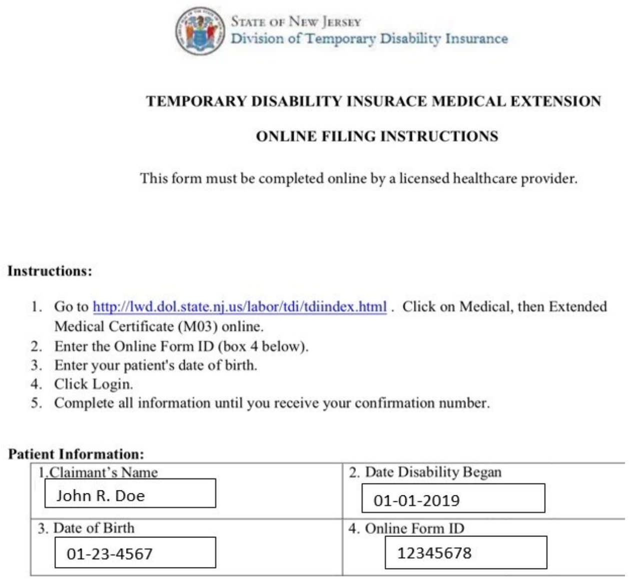
To help thousands of UNCHCS workforce members protect PHI effectively, we rely on those workforce members to contact us for guidance. This collaborative effort can help significantly reduce risk to the organization and to patient privacy. Next time your area is deciding on a workflow or process change in which there may be risks to PHI in the storage, transmission, access, use or disposal of that PHI, please give us a call (984-974-1069) or send us an email (Privacy@unchealth.unc.edu) and we will be happy to help.

UNC Health Care: Privacy Tips

Spotlight on Electronic Demands for Disclosure of PHI

Recently, providers have raised concerns regarding requests from patients to log-in through online portals to complete disability or FMLA paperwork. Such requests place the issues of security and privacy in question, which can quickly become a stumbling block for providers in their efforts to deliver the needed information for their patients' care.

Example 1: Emailed Request



State of New Jersey
Division of Temporary Disability Insurance

TEMPORARY DISABILITY INSURACE MEDICAL EXTENSION

ONLINE FILING INSTRUCTIONS

This form must be completed online by a licensed healthcare provider.

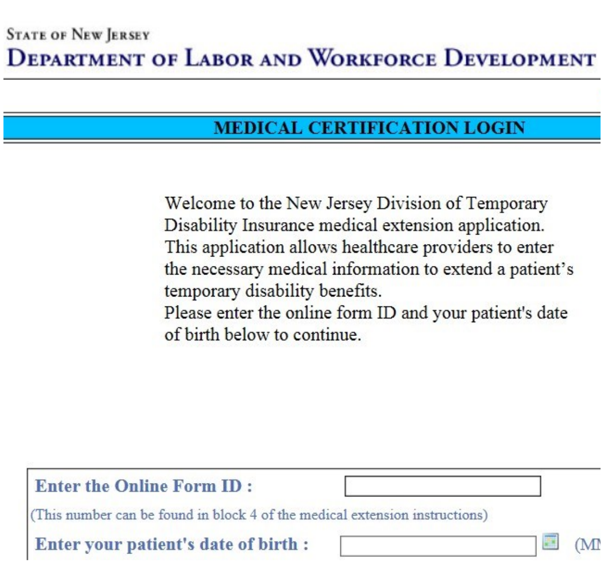
Instructions:

1. Go to http://lwd.dol.state.nj.us/labor/tdi/tdiindex.html . Click on Medical, then Extended Medical Certificate (M03) online.
2. Enter the Online Form ID (box 4 below).
3. Enter your patient's date of birth.
4. Click Login.
5. Complete all information until you receive your confirmation number.

Patient Information:

1.Claimant's Name John R. Doe	2. Date Disability Began 01-01-2019
3. Date of Birth 01-23-4567	4. Online Form ID 12345678

Example 2: Online Portal



State of New Jersey
Department of Labor and Workforce Development

MEDICAL CERTIFICATION LOGIN

Welcome to the New Jersey Division of Temporary Disability Insurance medical extension application. This application allows healthcare providers to enter the necessary medical information to extend a patient's temporary disability benefits.
Please enter the online form ID and your patient's date of birth below to continue.

Enter the Online Form ID :
(This number can be found in block 4 of the medical extension instructions)
Enter your patient's date of birth : (M

Here are a few guidelines to keep in mind while we navigate this electronic age we find ourselves in, and as we attempt to balance patient satisfaction in conjunction with patient privacy simultaneously:

1. **Verify the identity of a person requesting PHI** and the authority of any such person to have access to PHI, if the identity or authority of the requestor is not known by the workforce member.

2. **Obtain documentation of a written statement or request on official letterhead from the person or entity requesting the PHI** in order to ensure they are a legitimate requesting source as a condition of the disclosure.

3. **Verify the security of the online portal URL requesting the PHI.** Take the time to look at the requesting entity portal and look for secure identifiers such as individual ID numbers tied to that patient case within the official request. Please review the examples above.

The HIPAA Privacy Rule allows covered entities to rely on their professional judgment, as well as industry standards, in designing reasonable verification and authentication processes. Due diligence and use of the above guidelines help ensure the appropriate use and disclosure of patient PHI.

For more information regarding verification of identity and authority of individuals requesting PHI please review the UNCHCS Verification of Identity Policy.

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 Tips

Spotlight on Misdirected Documents

While we all try our best to avoid privacy incidents, the UNCHCS Privacy Office understands that accidents do happen. Many of the reports we receive involve paper documents that end up in the wrong hands. The most commonly reported incidents of this type occur when a patient is accidentally handed someone else's after visit summary or discharge summary. Even though this is often a result of a simple mistake, it is still an inappropriate disclosure of protected health information (PHI) that must be reported the UNCHCS Privacy Office.

When this type of incident has been identified, the Privacy Office must evaluate the information involved and determine the cause in order to help you minimize the possibility that it will happen again. As mentioned above, these incidents are often caused by employee error and can be resolved with retraining. However, a process within the department or clinic may also need correction to help reduce risk.

If you become aware of a situation involving a misdirected document, please remember the following steps:

1. **Contact the recipient** of the misdirected document and apologize for the incident. Remember to assure the recipient that UNCHCS takes patient privacy seriously and that his/her information is safe (as long as there is no reason to believe otherwise).

2. **Attempt to arrange the return of the document.** You can ask them to bring the document back to your location or offer to send a self-addressed, stamped envelope so they can easily return the document. If neither of these options is possible, ask the recipient to destroy/shred the document.

3. **File a Privacy Incident Report** through our online reporting tool (hotline.unchealthcare.org) or by calling the Hotline at 800-362-2921. In your report, please include as much as possible of the following information:
   a. Whose PHI was disclosed?
   b. What PHI was disclosed?
      - If possible, include a copy of the misdirected document in the report. You can attach a copy of the document through the online reporting tool.
   c. Who received the PHI?
      - Was it another covered entity or another patient? Be specific and provide as much contact information as you can.
   d. What is the disposition of the PHI?
      - Were you able to contact the recipient? Did they return the document or shred it?
   e. Can you determine how this occurred?
      - If you have identified the cause, what steps have been taken to minimize the possibility that this will reoccur? (i.e., staff retraining or modification of an internal process).