



Special points of interest:

- Understand how to report Privacy incidents
- 2016 HIPAA settlements
- Changes to the Confidentiality / Privacy / Information Security LMS module
- Record-breaking HIPAA settlement
- Best practices for sending inter-departmental mail
- UNC Health Care policy updates
- UNC Health Care: Privacy tips and FAQs

Inside this issue:

UNC Health Care: 2
2017 LMS
Module

\$5.5 Million 2
HIPAA
Settlement

UNC Health Care: 3
Inter-
Departmental
Mail

UNC Health Care: 4
Privacy Policy
Updates

UNC Health Care 4
FAQs: Identity
Theft

UNC Health Care: New Privacy Incident Reporting Process

In September, the UNC Health Care (UNC HC) Privacy Office implemented a new Privacy Incident Reporting process and has asked that all workforce members and employees use this process to communicate known or suspected privacy incidents to our office.

To file a Privacy Incident Report, first go to the [UNC HC Privacy Office intranet page](#) and click on the link located under the icon in the top right-hand corner. This will take you to the web page where you can download the fillable PDF Privacy Incident Report Form. Complete all fields on the form and save it to your work computer. Then, attach the completed form to a secure email and send it to: Privacy@unchealth.unc.edu. The UNC HC Privacy Office will contact you within ten (10) business days to discuss the matter and initiate an investigation, as appropriate.

The UNC HC Privacy Office team remains available by phone and email to answer any questions you may have about our Privacy Program or our Privacy policies.



Millions Paid in 2016 by Large Health Systems and Academic Medical Centers for HIPAA Violations

In 2016, the U.S. Department of Health and Human Services, Office for Civil Rights (OCR) entered into 11 separate resolution agreements, including several with large health systems and academic medical centers. The resolution agreements have required these 11 health care entities to pay resolution amounts totaling more than twenty million dollars (\$20,000,000). Both the [University of Mississippi Medical Center](#) and [Oregon Health Sciences Center](#) are two of the entities that have paid millions of dollars to OCR for HIPAA violations.

OCR has already entered into nearly as many resolutions agreements for HIPAA Privacy violations in 2016 as it did for the prior two years combined. OCR has indicated that it will continue to vigorously pursue enforcement actions against those entities that violate the HIPAA Privacy rules.

That is why our office would like to ensure that all employees across UNC Health Care are continuously and actively engaged in HIPAA compliance efforts and understand that the UNC Health Care Privacy Office (ph: 984.974.1069 / privacy@unchealth.unc.edu) and your facility's Privacy Officer are available to assist with any questions about compliance requirements with the UNC Health Care Privacy policies or HIPAA.

UNC Health Care: 2017 Confidentiality / Privacy / Information Security LMS Module

The UNC Health Care (UNC HC) Privacy Office would like to announce the roll-out of the new annual 2017 *Confidentiality, Privacy, and Information Security* training that will go-live on November 1.

When the LMS module is published in November, you will find that the UNC HC Privacy Office, in partnership with Information Security and others, has made updates to reflect recent changes to our internal policies and procedures. Some examples include:

- **Payment Card Industry (PCI) Compliance**, including requirements for those who handle credit card payments to properly secure that information.
- UNC Health Care is dedicated to a culture of **nondiscrimination**. The LMS module has been updated to reflect that commitment by clarifying that a patient's sexual orientation is confidential.
- The process for handling **subpoenas** has also been updated to direct any employee, who

receives a subpoena for patient information, to his/her facility's Health Information Management (HIM) office.

The 2017 module also includes an expanded look at the true cost of a privacy breach as seen in recent news headlines. The academic medical centers in these stories have been assessed significant fines for non-compliance and illustrate why your commitment to patient privacy is so important. Each member of our workforce is responsible for keeping patient

information safe by complying with all Privacy and Information Security policies. If you have any questions about these policies, please talk with your supervisor or contact our office or your facility's Privacy Office for assistance.

We are grateful for your continued commitment to the privacy and security of patient information.

Your feedback on 2017 training material is welcome and can be submitted by email to the UNC HC Privacy Office at Privacy@unchealth.unc.edu.



Record-Breaking \$5.5 Million HIPAA Settlement

On August 4, the Office for Civil Rights (OCR) [announced](#) that Advocate Health Care Network (Advocate) will pay \$5.5 million and adopt a corrective action plan to resolve potential HIPAA violations.

The settlement arose from a 2013 OCR investigation of three breaches, involving the electronic protected health information (e-PHI) of roughly four million individuals. The e-PHI included demographic information, clinical information, health insurance information, patient names, addresses, credit card numbers and their expiration dates, and dates of birth.

In the course of its investigation, OCR found that Advocate failed to:

- conduct an accurate and thorough assessment of the potential risks and vulnerabilities to all of its e-PHI;
- implement policies and procedures and facility access controls to limit physical access to the electronic information systems

housed within a large data support center;

- obtain satisfactory assurances in the form of a written business associate contract that its business associate would appropriately safeguard all e-PHI in its possession; and
- reasonably safeguard an unencrypted laptop when left in an unlocked vehicle overnight.

OCR said the settlement is "the largest to-date against a single entity" because of the extent and duration of the alleged noncompliance and the large number of affected individuals. "We

hope this settlement sends a strong message to covered entities that they must engage in a comprehensive risk analysis and risk management to ensure that individuals' ePHI is secure," said OCR Director Jocelyn Samuels. "This includes implementing physical, technical, and administrative security measures sufficient to reduce the risks to ePHI in all physical locations and on all portable devices to a reasonable and appropriate level."

Please review relevant policies including [ADMIN 0082](#) (Information Security).

UNC Health Care: Sending PHI in Inter-Departmental Mail

The UNC HC Privacy Office has recently investigated several incidences of Protected Health Information (PHI) being delivered via inter-departmental mail to a location other than what was intended by the sender. In some cases, PHI sent via inter-departmental mail has been delivered to recipients at the University of North Carolina at Chapel Hill, which is separate and

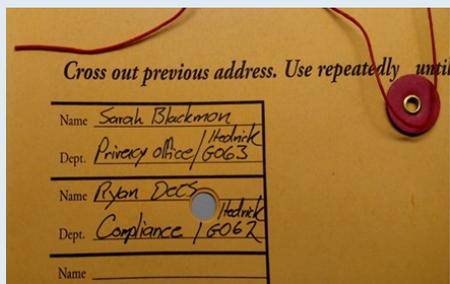
apart from UNC Health Care. In these instances, it appears that the inter-departmental envelopes were either not clearly addressed or addressed to more than one recipient.

If you absolutely must send PHI through inter-departmental mail, please be sure to clearly indicate where and to whom the inter-departmental mail

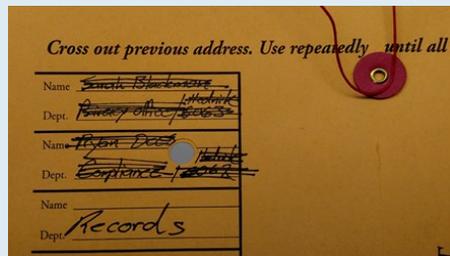
containing PHI should be delivered. Also, please verify and ensure that all previous recipients listed on the inter-departmental mail envelope are marked out. Sensitive patient information can be compromised if not delivered to the correct recipient. It is also highly recommended that the PHI be separately sealed in an envelope or other folder inside the inter-departmental envelope and that your name and contact information be included on that envelope or folder as well.

Please review the examples below of secure and unsecure inter-departmental mail.

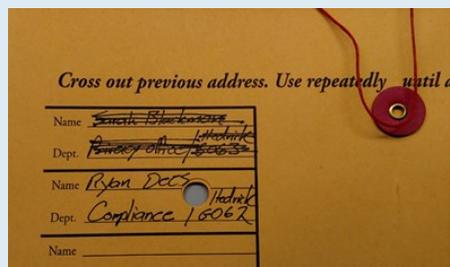
Inter-Departmental Mail Examples:



Unsecure
Sender did not cross out the names of previous inter-departmental mail recipients



Unsecure
Sender did not clearly specify the recipient (name, address) who will receive the inter-departmental envelope.



More Secure
The recipient's name and address are clearly indicated. The names of previous recipients have been marked out.

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](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**

UNC Health Care — Policy Updates

The following Privacy and Security policies were updated between July 1, 2016 and September 30, 2016:

HIPAA Manual (multi-entity)	Administrative Manual (UNC Medical Center)
<ul style="list-style-type: none">• ADMIN 0022 — HIPAA Business Associates Policy and Procedure	<ul style="list-style-type: none">• ADMIN 0097 — Medical Records Control (Paper-Based)• ADMIN 0168 — Shadow Students or Visitors• ADMIN 0175 — Suspected Child Abuse, Neglect, or Dependency

UNC Health Care: Privacy Tips and FAQs



Spotlight on Identity Theft

Below are some FAQs concerning identity theft

TIP: What is the Red Flag Program at UNC Medical Center?

ANSWER: *The Red Flag Program is concerned with detecting, preventing, and mitigating potential threats (“red flags”) posed by identity thieves using illicitly obtained personal information. The policy requires UNC Medical Center staff to report “red flags,” including but not limited to: suspicious documentation of identity, documents returned for bad address, use of the same Social Security number by multiple patients, and notification from patients, victims of identity fraud, law enforcement, and other credible sources regarding identity theft in connection with a UNC Medical Center account. For more information, please consult the [ADMIN 0202](#) (Identify Theft Prevention, Red Flag Program) policy.*

FAQ: Where can I find information about the Identify Theft Protection Act (ITPA)?

ANSWER: *Information about ITPA compliance is located in the Identify Theft Protection policy ([ADMIN 0088](#)) in the HIPAA Manual.*

FAQ: Do you have any handouts on identity theft?

ANSWER: *Yes! Please review the Identify Theft Resources [handout](#) on the Privacy Office Intranet site.*

HIPAA Manual Reference: [ADMIN 0088](#) (Identify Theft Protection)

UNC Medical Center Policy Reference: [ADMIN 0202](#) (Identify Theft Prevention, Red Flag Program)