New Hanover Regional Medical Center
Pender Memorial Hospital
an affiliate of New Hanover Regional Medical Center

Compliance CAPSULES

Vol. 12 No. 4, September 2018

HIPAA SETTLEMENTS AFTER UNAUTHORIZED DISCLOSURE OF PATIENTS' PROTECTED HEALTH INFORMATION (PHI) WHILE FILMING

On September 20, 2018, the Department of Health and Human Services, Office for Civil Rights (OCR) announced that it has reached separate settlements with Boston Medical Center (BMC), Brigham and Women's Hospital (BWH), and Massachusetts General Hospital (MGH) for compromising the privacy of patients' protected health information by inviting film crews on premises to film an ABC television network documentary series, without first obtaining authorization from patients.

Collectively, the three entities paid OCR **$999,000** to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule.

"Patients in hospitals expect to encounter doctors and nurses when getting treatment, not film crews recording them at their most private and vulnerable moments," said Roger Severino, OCR director. "Hospitals must get authorization from patients before allowing strangers to have access to patients and their medical information."

In addition to the penalties, each hospital is subject to a corrective action plan requiring each to revise policies and train staff. A FAQ on the OCR's website: **"Can health care providers invite or arrange for members of the media, including film crews, to enter treatment areas of their facilities without prior written authorization?"** In its response, OCR instructs that, for non-public areas of a hospital, a written authorization is required "from each individual who is or will be in the area or whose PHI otherwise will be accessible to the media."

This is an excellent reminder that providers must be vigilant in protecting PHI, ensuring patients sign authorizations before making any disclosures.

Source: HHS.gov - HHS Press Office Release

Corporate Compliance Hotline:
1.800.348.9847 or
www.MyComplianceReport.com
Access ID: "NHR"

WOULD YOU TAKE A PICTURE?

With NHRMC's continual implementation of the latest and greatest in medical innovation to benefit our patients, the risk of pictures of patients being used in news stories is increasing.

A potential scenario might be: A news story about a new intervention available at NHRMC has been arranged. You are asked to take a picture of the patient during the new procedure. Would you assume all aspects of our Consent to Photograph Policy have been followed and take the picture?

BEFORE YOU TAKE A PICTURE

Before taking a patient's picture, be sure you know how the picture will be used and follow the Consent to Photograph/Video/Interview policy.

If the patient's picture will be used for media release, be sure NHRMC Marketing and Public Relations staff are aware and have worked with the media representatives to ensure the patient's rights are protected.

SECURITY

Personal devices, including cellular phones are ONLY permitted for patient documentation and photographs if one is using an approved NHRMC secure mobile application on their device.

MEDIA REQUESTS – PROCEDURE

- Media representatives should work with NHRMC's Marketing and Public Relations Office to arrange for permission from appropriate parties and should be escorted by a representative or designee of the NHRMC Marketing and Public Relations office. No photograph, file or video in which a patient is identifiable should be taken without the prior written authorization of the patient or the patient's authorized representative.
- When a patient or visitor is to be photographed, videoed, audio-recorded or interviewed for the purposes of release to the public, there should be a Consent to Photograph/Video/Interview form (NS-1709) completed.

MEDIA REQUESTS – PROCEDURE (CONT'D)

- A copy of the completed consent is to be placed in the patient's medical record and a copy will be kept in the Marketing and Public Relations office.
- The patient has the right to rescind consent up until the time the photographs, video, motion picture, voice/sound recordings and/or interview are taken. Once made public, revocation may not be possible.
- The Marketing and Public Relations staff will communicate the request to rescind consent to the media.
- At any time, the patient's physician, nurse or public relations representative can require that the photographing, taping or recording be discontinued.
- If the photographs, videos, voice/audio recordings or interviews are shared with a third party, this will be documented on the Consent to Photograph/Video/Interview and Authorization to Use/Disclose form (NS-1709).

POLICY QUESTIONS

Consent to Photograph/Video/Interview policy is on PolicyStat. For questions or situations not covered by the policy, contact Marketing and Public Relations or Risk Management for guidance.

HIPAA STATS, July – Sept 2018

	Violations	Inadvertent Breaches
NHRMC & PMH/HC	3	13
NHRMC PG	1	1
Business Partners	0	1

HIPAA violations are addressed according to the HR Policy, "Progressive Discipline."

IDENTITY THEFT, SSN & PERSONAL IDENTIFYING NUMBERS

According to the Social Security Administration, identity theft is one of the fastest growing crimes in America. Identity theft affects millions of Americans every year, and the Social Security Number (SSN) is a key that thieves use to unlock many forms of identity fraud.

Proprietary business information and patient identifiable health information are both considered "confidential information." As NHRMC employees it is our responsibility to safeguard the privacy of all patients and to protect the confidentiality of our patient's health information. It is also our legal and ethical responsibility to safeguard a patient's business information, such as Social Security numbers or credit card information.

In accordance with the North Carolina Identity Theft Protection Act of 2005 and the Federal Trade Commission's Red Flag Rules, it is the policy of NHRMC and its affiliates, to protect the privacy and integrity of consumers' personal information and prevent unauthorized use or disclosure.

IDENTITY THEFT, SSN & PERSONAL IDENTIFYING NUMBERS (CONT'D)

NHRMC's Identity Theft Prevention and Protection policy, provides guidance on the appropriate uses and disclosure of consumer's personal information and meeting legal obligations under law.

Collection, use and disclosure of SSNs and other personal identifying numbers:

- Do not collect a SSN unless you are authorized to do so or the SSN is imperative to perform NHRMC's duties and responsibilities.
- Segregate SSNs on a separate page from the rest of the record.
- Provide the individual, upon request, with a statement of the purpose for the SSN being collected and used.
- Do not use the SSN for any purpose other than the purpose stated.
- Do not intentionally communicate or make available to the public a person's SSN or other identifying number.
- Do not intentionally print or imbed an individual's SSN on a card for the individual to access government or NHRMC products or services.

IDENTITY THEFT, SSN & PERSONAL IDENTIFYING NUMBERS (CONT'D)

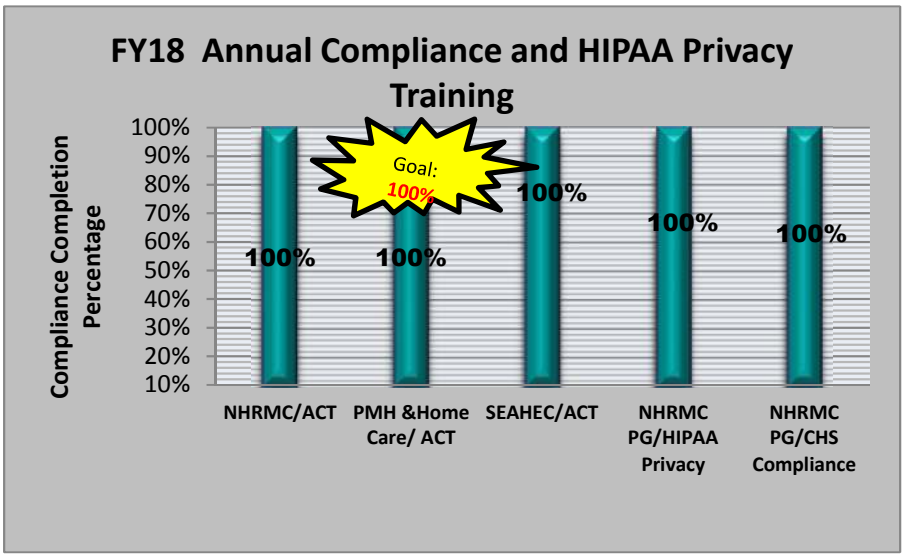
- Do not require an individual to transmit their SSN over the Internet, unless the connection is secure or the SSN is encrypted.
- Do not require individuals to use their SSN's to access an Internet Web site, unless a password or unique personal identification number or another authentication device is also required to access the Internet Web site.
- Do not print an individual's SSN on any materials mailed to the individual, unless state or federal law requires the SSN be on the document being mailed; no postcards or visible SSNs on unopened mail.
- Do not sell, lease, loan, trade, rent, or intentionally disclose an individual's SSN to a third party without written consent from the individual, when the party making the disclosure knows or has reason to believe that the third party lacks a legitimate purpose for obtaining the individual's SSN.

Source: Identity Theft Prevention and Protection (Corporate Policy), PolicyStat

Compliance CAPSULES

ANNUAL COMPLIANCE & PRIVACY EDUCATION FY 2018

FY 2018 mandatory computer-based learning modules were due for completion **by August 1, 2018.** FY18 completion rates for compliance and privacy modules will be reported to the Compliance Committee and the Audit & Compliance Committee of the Board.



COMPLIANCE QUIZ FOR MOVIE TICKETS

Email Your Responses to Stephanie Snyder by October 31, 2018

1. Providers must be vigilant in protecting PHI, ensuring patients sign _____ before making any disclosures.
2. Proprietary business information and patient identifiable health information are both considered _____.
3. The _____policy addresses when a patient's picture is to be used for media release.
4. Media representatives should work with NHRMC's _____ Office.
5. Do not collect a _____unless you are_____ or the _____is imperative to perform NHRMC's duties and responsibilities.

Congratulations to Jennifer Sides, winner of movie tickets for the June 2018 newsletter!

"Science brings SOCIETY to the next level; ETHICS keeps us there."
Dr. Hal Simeroth