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

Compliance CAPSULES

Vol. 14 No. 1, December 2019

IS SANTA BRINGING YOU A SMARTWATCH?

The Stop Marketing And Revealing The Wearables And Trackers Consumer Health (SMARTWATCH) Data Act, has been introduced by Sens. Bill Cassidy, M.D., (R-Louisiana) and Jacky Rosen, (D-Nevada). The new legislation will ensure that health data collected through fitness trackers, smartwatches, and health apps, cannot be sold or shared without consumer consent.

Q: Why the need for new legislation when we already have the Health Insurance Portability and Accountability Act (HIPAA)?

A: Because HIPAA applies to health data collected, received, stored, maintained, or transmitted by HIPAA-covered entities and their business associates.

Consumer devices are defined as "equipment application software, or mechanism that has the primary function or capability to collect, store, or transmit consumer health information."

However, some of the same information, is collected, stored and transmitted by fitness trackers, wearable devices, health apps, but is not protected under HIPAA.

WHAT'S THE RISK?

Currently, that information can be used, shared, or sold, without consent. Consumers have no control over who can access this health data. The new legislation aims to address this **privacy gap.**

The bill prohibits the transfer, sale, sharing, or access to any non- anonymized consumer health information or other individually

IS SANTA BRINGING YOU A SMARTWATCH? (CONT'D)

identifiable health information that is collected, recorded or derived from personal consumer devices to domestic information brokers, other domestic entities, or entities outside the United States, unless consent has been obtained from the consumer.

WHAT WILL THE SMARTWATCH DATA ACT PROTECT?

The Smartwatch Data Act applies to information about the health status of an individual, personal biometric information, and kinesthetic information collected directly through sensors or inputted manually into apps by consumers. The Smartwatch Data Act would treat all health data collected through apps, wearable devices and trackers, as protected health information!

IS THIS AN EXTENSION OF HIPAA?

No. While in the past, there have been requests for HIPAA to be extended to cover app developers and wearable device manufacturers that collect, store, maintain, process and transmit consumer health information, this Act does not extend HIPAA to cover these companies. Instead, the legislation applies to the data itself.

However, the bill proposes that the HHS' Office of Civil Rights (OCR), the main enforcer of compliance with HIPAA, be responsible for enforcing compliance with the Smartwatch Data Act. The **penalties** would be the same as the penalties for HIPAA violations.

BRIEFLY- ON OCR PENALTIES

The OCR currently has the power to issue financial penalties and/or corrective action plans to covered entities that fail to comply with HIPAA. Monetary penalties are intended to act as a deterrent to prevent HIPAA violations, while also ensuring covered

IS SANTA BRINGING YOU A SMARTWATCH? (CONT'D)

entities are held accountable for their failure to protect the privacy of patients and confidentiality of health data. The penalties have ranged from the largest-ever to date in 2018 of **$16 million** to an average of approximately ***$1.7 million*** in the last 3 years.

The introduction of technology to our healthcare system in the form of apps and wearable health devices has brought up a number of important questions regarding data collection and privacy," said Sen. Rosen. "This commonsense, bipartisan legislation will extend existing health care privacy protections to personal health data collected by apps and wearables, preventing this data from being sold or used commercially without the consumer's consent."

WHY THIS LEGISLATION NOW?

The legislation was introduced following the news that Google had partnered with Ascension, the second largest healthcare provider in the United States, and has been given access to the health information of 50 million Americans. That partnership has raised many questions about the privacy of health information.

While the Ascension data passed to Google is covered by HIPAA, currently, fitness tracker data is not. In addition, Google plans to acquire fitness tracker manufacturer Fitbit in 2020, leading to concern about how Google will use personal health data collected from Fitbit devices. This new Act would help ensure consumers are given a say in how their health data is used!

Source: HIPAA Journal, 11.21.19, "Smartwatch Data Act Introduced to Improve Protections for Consumer Health Data"; Stats source - JDSURPA article, Feb. 27, 2019 "HIPAA Compliance for 2019: Enforcement Trends and Lessons Learned from 2018."

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

.

MAKING HIPAA STICK!!

Lots of articles are written with a focus on HIPAA, privacy regulations, and the importance of these policies being current in healthcare organizations. The importance of staff education and awareness is equally important. However, a recent article made an excellent and profound point!

HIPAA policies become truly meaningful when daily activities in the organization and the goal of keeping health information a secret to all except those who need to know, is owned by everyone! ***In other words, HIPAA ownership STICKS!***

CONFIDENTIALITY-A BOND OF TRUST

For effectiveness of education, policies, procedures, etc., the daily procedures must align naturally with policy expectations, less because of the rules and more because of shared values that uphold **confidentiality as a bond of trust.** With this mindset in staff, there is sensitivity to potential harm to people's lives when private information gets out. **Example:** The unwanted disclosure of paternity results or a chronic disease, etc., can tear apart relationships or derail careers.

MAKING HIPAA STICK!! (CONT'D)

CONFIDENTIALITY - A BOND OF TRUST (CONT'D)

Information shared with anyone without a need to know to perform their job duties can prove devastating and/or life changing. It is our belief that no one in this organization would ever intentionally hurt a patient!

NO ONE IS EXEMPT

This truth applies to all, regardless where we work in the organization. **Consider this:** We put a baby in a car seat, not just because it's the law, but we do it to protect the child and couldn't imagine not doing it! Similarly, we protect patient privacy, not just because it's the law, but because they trust us to do so!

TOOLS FOR SUCCESS

The need for good HIPAA policies and procedures, ongoing education and monitoring is a must! These equip staff to understand confidentiality in the terms of **a bond of trust** and HIPAA then simply becomes a means to the desired end!! Policies stick because our organization is trusted and we intentionally keep secrets entrusted to us by our patients.

MAKING HIPAA STICK!! (CONT'D)

WE ARE BETTER AND CAN LEAD

Recently, a list of the top 10 most common HIPAA violations was published: **#1 - SNOOPING!**

Employees snooping in records of family, friends, neighbors, co-workers, etc., often ending in termination & some in criminal charges. Lead by respecting the **bond of trust!** Don't be a stat!

Sources: The Compliance & Ethics Blog, 6.10.19, "Make HIPAA Stick! Privacy Officers, Set the Table for Everyday Vigilance") (Stats-HIPAA Journal, 4.26.19, "The Most Common HIPAA Violations You Should Be Aware Of".

HIPAA STATS, Oct. – Dec. 2019

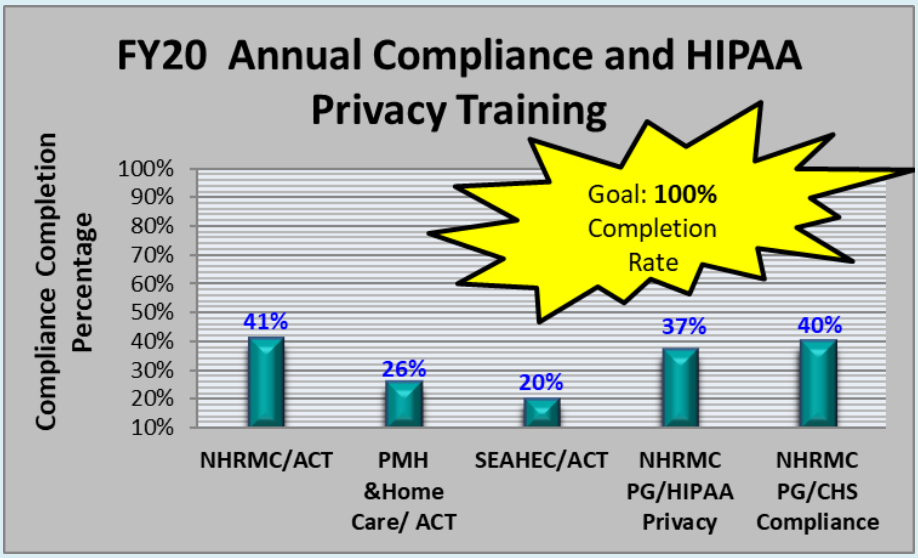
	Violations	Inadvertent Breaches
NHRMC & PMH/HC	**12**	**12**
NHRMC PG	**0**	**6**
Business Partners	**0**	**1**

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

Compliance | CAPSULES

ANNUAL COMPLIANCE & PRIVACY EDUCATION FY 2020

FY 2020 mandatory computer-based learning modules are due for completion **by August 1, 2020.** FY20 completion rates for compliance and privacy modules were reported to the Compliance Committee and the Board.



COMPLIANCE QUIZ FOR MOVIE TICKETS

Email Your Responses to Stephanie Snyder by January 31, 2020

1. The SMARTWATCH legislation has been passed into law. (True or False) _____
2. The _____ will ensure that health data collected through fitness trackers, smartwatches, and health apps, cannot be sold or shared without consumer consent.
3. The bill proposes that the_____, be responsible for enforcing compliance with the Smartwatch Data Act.
4. Confidentiality should be viewed as a _____ we have with our patients.
5. The #1 HIPAA violation recently published in the list of top ten was _____.

Congratulations to Melissa Gutierrez, winner of movie tickets for the September 2019 newsletter!

"It isn't what we say or think that defines us, but what we do."

-Jane Austen