HIPAA Guard HERALD
YOUR MONTHLY NEWSLETTER ON SURVIVING HIPAA

ISSUE 05 April 2018

LATEST ON HIPAA

HIPAA Violations by Employees Resulted in Jail Terms

When Employees Illegally Accessed Patient Files

Employees accessing patient information when they are not authorized is another very common HIPAA violation. It could be out of curiosity, malice, or as a favor for a relative or friend, this is illegal and can cost a practice greatly. Also, individuals that use or sell PHI for personal gain can be subject to fines and even imprisonment. This is exactly what transpired to the Transformations Autism Treatment Center (TACT), in Bartlett, Tennessee. One of its employees, a behavioral analyst, Jeffrey Luke, was terminated. And like every covered entities, the company in compliance with HIPAA law terminated its employee's access to sensitive data and changed the email address authorized to access its data. Nonetheless, about 300 current and past patient clients of TACT has been accessed via Google Drive and later on found out to have been accessed remotely by the terminated employee. It was also discovered this was not the first time Luke had stolen data from an employer. His computer also contained records of a former employer, Behavioral and Counseling Services (BCS) in Somerville, Tennessee. These records also contained patient data.

Luke went on to plead guilty to the crime and was sentenced to 30 months' imprisonment and three years' supervised release, and he was ordered to pay approximately $15,000 in restitution. It is possible that one account has access and shared by multiple users. This shared credential is a mortal sin to information security. A unique access requiring individual login to the patient data stored via cloud storage is more secured than a shared email account.

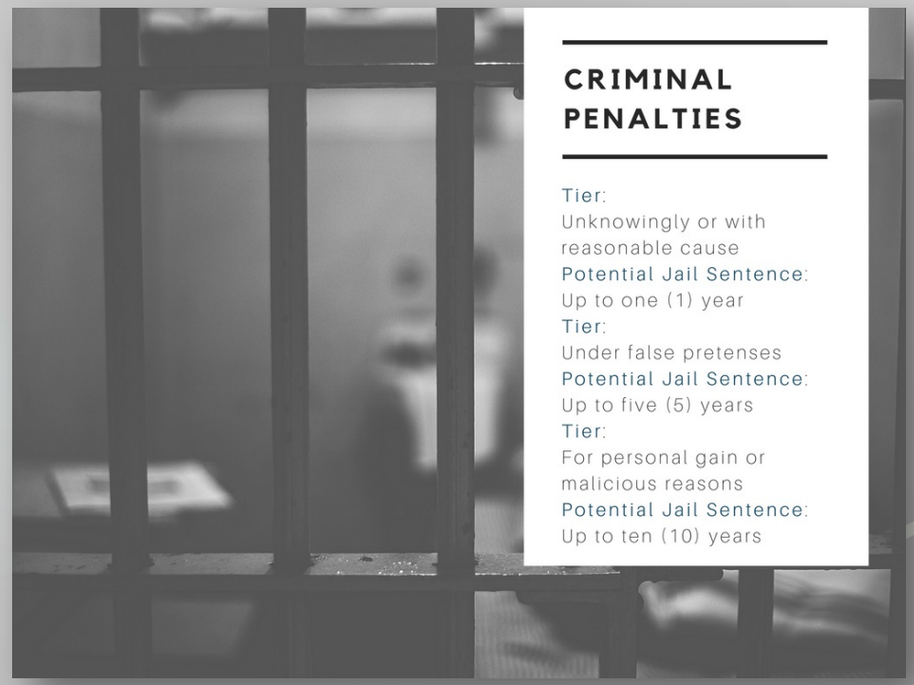
The lesson here is that healthcare employees considering stealing healthcare data to sell, use, or pass on to a new employer, that data theft carries rigid penalties. While Luke will only serve 30 days in jail, he will have a criminal record which will impede future employment. Another recent employee violation that suffered huge fines is the case of a nursing home employee, Shaniece Borney, 29, of St. Louis County, a former employee of NHC Health Care nursing home between 2016 and 2017. She stole the credit card details of patients to make purchases for herself and family members. The said employee faces up to 10 years in jail and could be fined up to $250,000 and will be required to pay restitution to the victims of the fraud. Verdict will be read on June 21, 2018.

Reference:

42 U.S.C. § 1320d-5 covers civil violations

42 U.S.C. § 1320d-6 covers criminal violations

These sections are not found in the HHS Regulations, rather they are Congressionally promulgated statutes found in the U.S. Code.



Role-Based Access Control (RBAC)

The Need for RBAC

It must be established that the need for RBAC stems from the HIPAA Privacy Rule's minimum necessary provisions.

HIPAA Privacy requires that covered entities provide workers with access to **only the minimum necessary information** needed to perform their work, given their particular role in the organization. The most effective way to do this is **role-based access control**.

Setting Up RBAC

So how do we go about establishing Role-Based Access Controls?

1. **Define the Roles**

Conduct a survey among management and staff to determine what resources and data they need to access to do their job. You may then categorize users who have similar access needs. Then match each role to a collection of resources i.e. systems, programs, applications, software, files, and data fields. These roles must be reviewed and updated regularly to address complexities of different and certain roles. Determine the number of roles as well which depends on business needs. The more roles , the harder it will be to maintain, but having few roles won't guarantee security as well

2. **Make a list and inventory of all active applications of data**

Data may be grouped into various **types** (clinical, administrative, financial) and according to **sensitivity** (records pertaining to HIV, abortion and mental health might have stricter access requirements than any other patient records).

3. **Identify resources & possible limitations**

One good example is the ITC and HR Departments. ITC Department shall be responsible for the development and production of applications whereas the HR Department might be assigned to do data collection and processing.

4. **Establish audit and maintenance of RBAC**

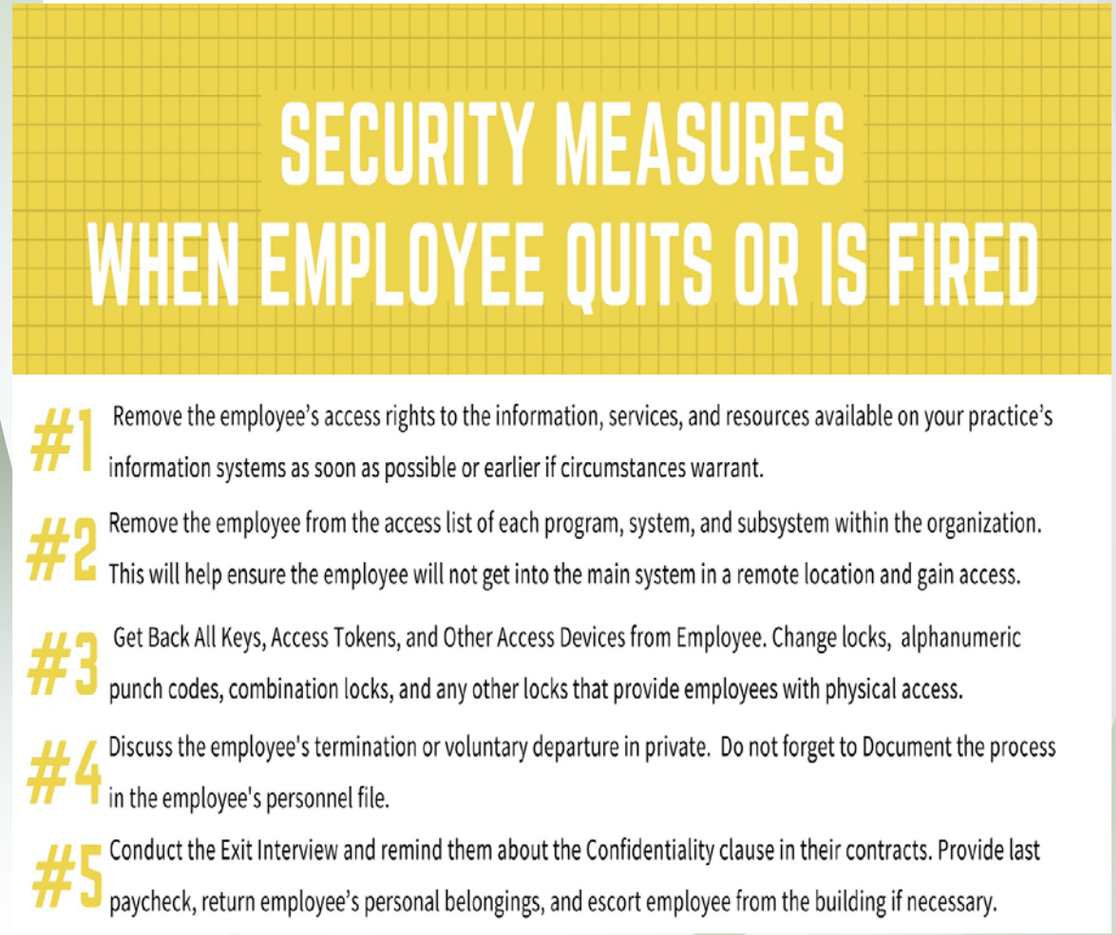
This is a very important factor to confirm that access is being controlled according to the organization's policies as roles, users, applications, files and policies change and of course, for ascertaining compliance with HIPAA and other regulations.

HR Role on HIPAA Compliance

Most organizations are overlooking the key component Human Resources (HR) should play in any compliance program. Human Resources team has the pivotal role in creating a culture of compliance in an organization. They are the bridge between the IT's functions in ensuring HIPAA compliance procedures are in place with the workforce who are the active participant in protecting PHI and ePHI.

In what areas HR team help in terms of ensuring HIPAA compliance is implemented and monitored?

1. *HR help screen and designate a Privacy Officer or Compliance Officer. They help ensure that a qualified, organized and responsible individual is put in these roles.*
2. *Maintain Policies & Procedures. HR Team are the ones responsible on concerns about employee termination, leave of absence, sanctions on non-completion of HIPAA related trainings and more. Once policies and procedures on concerns like these mentioned above are documented, these policies and procedures should be regularly updated and reviewed.*
3. *Application of Minimum Necessary Principle in giving access to onboarding employees and limit access to PHI to only cover areas needed or within the scope of their role.*
4. *Facilitate and Organize HIPAA Trainings for all staff and Management. Human Resources are the ones responsible for ensuring everyone in the organization gets the required HIPAA training (technical and awareness) so they know how they would fulfill their roles and prevent HIPAA violations. These type of trainings can be written in employment contracts as required trainings that the personnel must complete.*
5. *Human Resources are al responsible on creating and implementing proper exit procedures and process of resigning and terminated employees. Here are some of the steps HR must take when an employee leaves the company:*



UPCOMING

For tips and/ or training on any of these areas,

contact HIPAA Guard-

your partner in day to day HIPAA Compliance.

ISSUE 05
April 2018

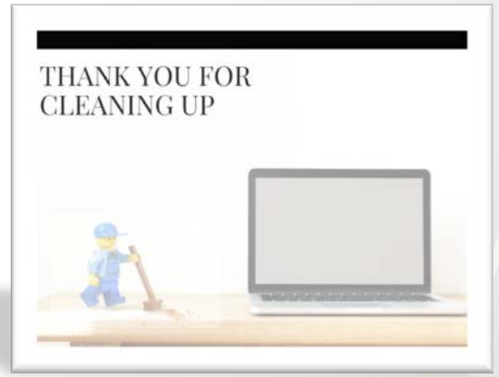
Asset Control Tags

IT make inventory of all assets within site, and tag them with specific numbers.

Make a form and process for this task, repeat annually. Any new devices, software, etc. will be tagged as it arrives on site.

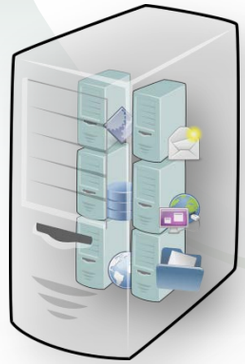
Log PHI Movement

PO needs to keep a log of where PHI is moved (in conjunction with IT).



Clean Up Workstations

Put nothing on desktops, secure files only, etc.



Delete Cloud-based Applications

Delete all Chromebook (and cloud based applications, devices)