HIPAA Guard HERALD

YOUR MONTHLY NEWSLETTER ON SURVIVING HIPAA

ISSUE 06 May 2018

LATEST ON HIPAA

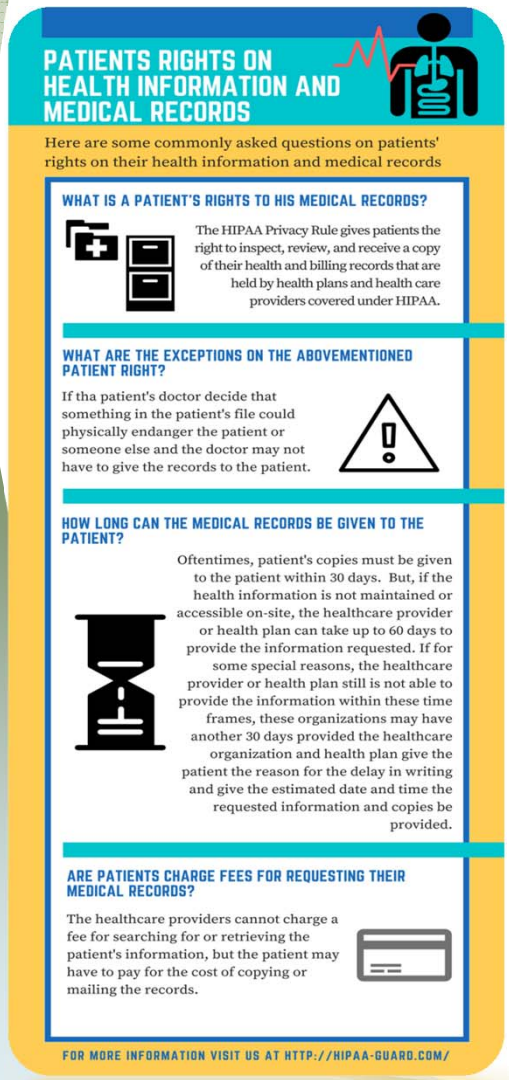
Three facilities of California-based Center for Orthopaedic Specialists attacked by Ransomware

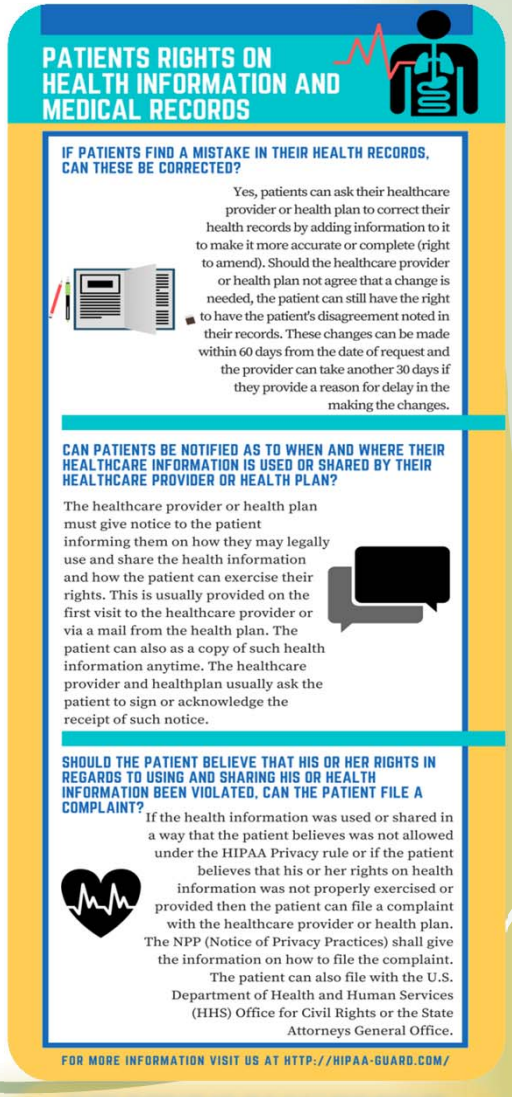
The Center for Orthopaedic Specialists (COS) has announced via its own website last April 18, 2018 that their computer system has been compromised that affected three of their facilities namely West Hills, Simi Valley and Westlake Village California. Malicious software was used to gain access to and encrypt patient data in the hopes of COS to pay money to restore access to the patient data. It was however reported that no patient information was removed by any unauthorized party as a result of this incident. This event was brought to the attention of COS by their third party technology vendor which provides COS with IT services. According to the investigation conducted by the third party vendor and COS, the unauthorized party began the attempt to access the COS system last February 18, 2018.

Source: http://www.cos-orthopaedics.com/web-notice/

The IT vendor indicated that the affected system was permanently taken offline before any patient information could be removed by the unauthorized party. It is believed that the patient data that was encrypted could have included patient's name, date of birth, details about their medical records, and Social Security number. But none was downloaded or removed by the unauthorized party according to the IT vendor and COS investigations. Notification has been sent to the federal enforcement officials who might need to conduct investigation on the matter. COS have arranged to have ID experts provide identification protection services for 24 months at no cost to their patients. The service is optional but strongly recommended to patients to take advantage of the benefits.

Patients Rights on Health Information and Medical Records

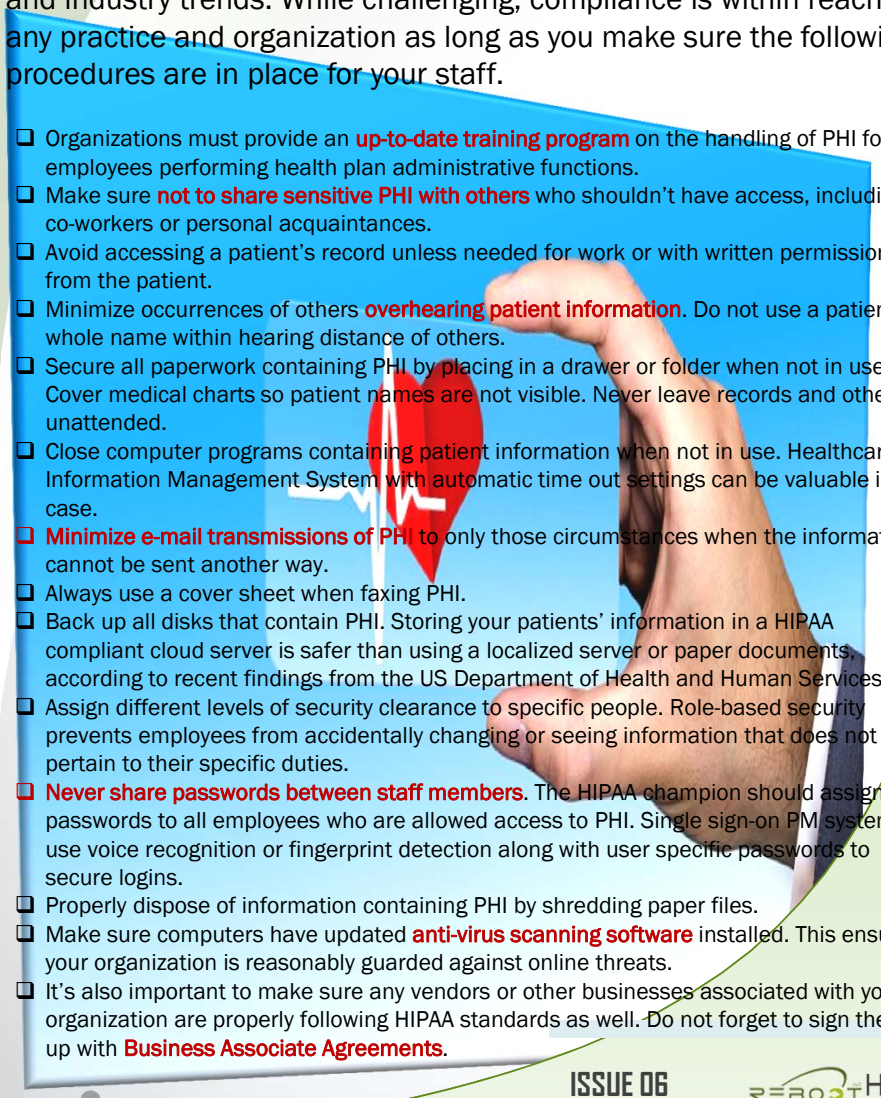




MORE ON **HIPAA Guard HERALD**

HIPAA Compliant Practices for your Staff

HIPAA standards are ever evolving to keep up with new technology and industry trends. While challenging, compliance is within reach for any practice and organization as long as you make sure the following procedures are in place for your staff.



- Organizations must provide an **up-to-date training program** on the handling of PHI for employees performing health plan administrative functions.
- Make sure **not to share sensitive PHI with others** who shouldn't have access, including co-workers or personal acquaintances.
- Avoid accessing a patient's record unless needed for work or with written permission from the patient.
- Minimize occurrences of others **overhearing patient information**. Do not use a patient's whole name within hearing distance of others.
- Secure all paperwork containing PHI by placing in a drawer or folder when not in use. Cover medical charts so patient names are not visible. Never leave records and other PHI unattended.
- Close computer programs containing patient information when not in use. Healthcare Information Management System with automatic time out settings can be valuable in this case.
- **Minimize e-mail transmissions of PHI** to only those circumstances when the information cannot be sent another way.
- Always use a cover sheet when faxing PHI.
- Back up all disks that contain PHI. Storing your patients' information in a HIPAA compliant cloud server is safer than using a localized server or paper documents, according to recent findings from the US Department of Health and Human Services.
- Assign different levels of security clearance to specific people. Role-based security prevents employees from accidentally changing or seeing information that does not pertain to their specific duties.
- **Never share passwords between staff members**. The HIPAA champion should assign passwords to all employees who are allowed access to PHI. Single sign-on PM systems use voice recognition or fingerprint detection along with user specific passwords to secure logins.
- Properly dispose of information containing PHI by shredding paper files.
- Make sure computers have updated **anti-virus scanning software** installed. This ensures your organization is reasonably guarded against online threats.
- It's also important to make sure any vendors or other businesses associated with your organization are properly following HIPAA standards as well. Do not forget to sign them up with **Business Associate Agreements**.

ISSUE 06
May 2018

REBOOT HIPAA GUARD

Role-Based Access Control for HIPAA Security

Everyone has his or her own role at an organization. The receptionist checks patients in. The nurse takes the vital stats of the patients. The physician diagnosis and determines treatment for the patient. The surgeon operates on the patient. What would happen if the receptionist just decided to switch roles with the surgeon for a day?

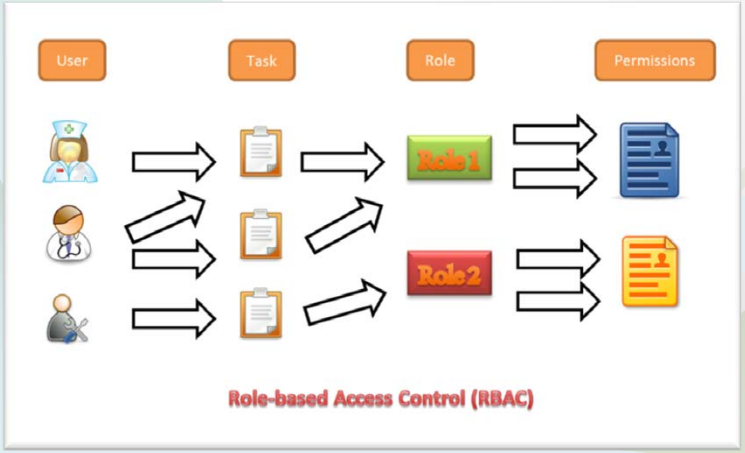
The same idea applies to PHI access across an organization, HIPAA Security Rule termed it as **Access Control (§ 164.312(a)(1))**. The Security Rule defines **access**:

> "…the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource

Healthcare organizations are mandated by federal law to make sure those with access to ePHI require that access to adequately do their jobs.

> "…Access controls should enable authorized users to access the minimum necessary information needed to perform job functions…"

One of the best ways of correctly setting up user privileges is by role and this is what we usually term as "**Role-based Access Control**".



Role-Based Access Control for HIPAA Security

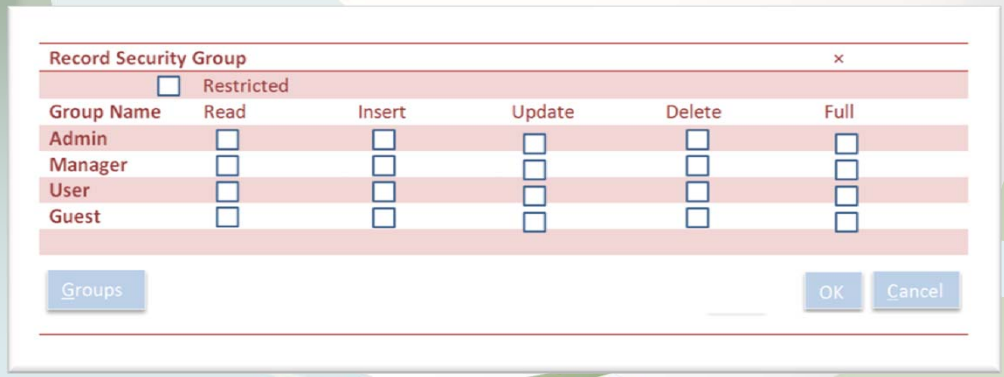
There are two ways to implement RBAC System:

- Electronic systems: Assignment of unique user ID is a great way to segment users by role and simplifies IT tracks user activity.
- Physical: Make sure anyone not on your regular staff is escorted around the office by a staff member and they should be wearing proper badges for easy identification. For patients, don't leave them unattended with logged-in equipment. For everyone else, document their name, reason for being at your organization, what company they're from, and what they look like. If you haven't worked with this person before, call the company and verify their name and physical description.

Implementing RBAC system is one that is full of challenges. There is a big investment of time and effort that is required in populating the RBAC matrix. The combination of locations, departments, employee types and roles – and the access rights they should be entitled to — can require a huge start up effort to accurately define. This is where the role of the Human Resources (HR) plays in. It is an excellent source for determining these combinations. Later we dig dipper on the big role the Human Resources play in the overall drive to HIPAA Compliance.

Permissions Settings Example

Here is a simplified 4-step approach in implementing an RBAC System:



HR's Role in HIPAA Security Compliance

Implementing RBAC system is one that is full of challenges. There is a big investment of time and effort that is required in populating the RBAC matrix. The combination of locations, departments, employee types and roles – and the access rights they should be entitled to — can require a huge start up effort to accurately define. This is where the role of the Human Resources (HR) plays in. It is an excellent source for determining these combinations. Later we dig dipper on the big role the Human Resources play in the overall drive to HIPAA Compliance.

Here are some of the HR tasks that are relevantly connected to attaining HIPAA Security Compliance:

1. Selection of a HIPAA Security Official

Covered entities are required to designate a single person to be ultimately responsible for the security of electronic PHI. Because of the technical issues involved, this professional should likely be someone other than the Privacy Officer. ITC managers may have the technical skills and the authority to select rightful candidate for the Security Officer role, HR professionals can give crucial guidance in choosing the right fit among the shortlisted candidates. HR can assess who among the candidates have the best potential to lead and manage or who will effectively interact with the employees and other members within the organization to accomplish the goals set for Security Rule compliance.

2. Assistance on RBAC System Set Up and Implementation

IT Department can program software to implement access controls on a technical level but it will be the HR's duty to identify for the IT Department those staff and management who are authorized to access PHI and ePHI as well as the scope of that access. Then once the RBAC system been set up, HR is still needed in ensuring proper implementation via proper initiation of training and awareness to staff and management of the importance of RBAC and the role each one has in complying with the policies and procedures set for their respective accesses in the system , files and facilities. In coordination by each department's managers and supervisors, HR will need to catalogue for the IT Department the categories of electronic PHI stored and transmitted by the organization and how the information is used and disclosed on the network to perform plan administration functions. HR will also have to assist the IT Department in developing access control lists as well as the types of access that will be permitted, e.g., read only, create new files, modify or delete existing files, search files, change security settings for specific files, etc. The list will be monitored and should there be any updates, HR will need to communicate accordingly to the IT Department (e.g. when employee is terminated, resigns, promoted or on a long leave of absence).

3. Development and Implementation of Written Policies

These processes and procedures are mandated to be documented and written policies be created for them as well as part of HIPAA compliance. HR will again be heavily involved in creating such policies:

- appropriate access to ePHI, including proper handling of terminated employees;
- Training, awareness & orientations;
- identifying, reporting, investigating and responding to security incidents;
- sanctioning employees for security violations; and
- proper data disposal, which would include the handling of electronic resources used by terminated employees.

HR's Role in HIPAA Security Compliance

4. Collaboration in Developing Security Awareness Training

Together with the Security Officer and IT Department, the HR shall collaborate with them in developing Security Awareness Training for the staff and management of the heathcare organization. Furthermore, HR shall be consulted in matters related to the following:

- identifying the employees who will need to undergo technical & awareness training,
- deciding whether new employees will be permitted to access electronic PHI before completing training,
- scheduling these training sessions, and
- documenting employee participation in those sessions
- Deciding whether current employees will be needing 'refresher courses' or any additional training for updates and changes affecting security compliance e.g. new application software, new system protection installations etc.

UPCOMING

De-identify PHI on Documents and X-rays
Maintain Documents for 6 years
Train Intake Employees
Train People Who Confirm Appointments

UPCOMING

Top 4 HIPAA Initiatives for the month of May 2018

Maintain Documents for 6 Years

HIPAA Rule Section 164.316(b)(1) mandates "*(i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) if an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.*" While Section 164.316(b)(2)(i) goes on to state: "*Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.*"

You should be maintaining all of your policies and documentation that address aspects of HIPAA, and you should plan to retain it all for 6 years at a minimum. You should also maintain all risk assessments, audits, and other documentation related to your organization.

For tips and/ or training on any of these areas, contact HIPAA Guard-

your partner in day to day HIPAA Compliance.

ISSUE 06
May 2018

REBOOT HIPAA GUARD

De-identify PHI on documents and X-rays

There are two methods that can be used to for de-identification of protected health information on documents and X-rays namely :

- Expert Determination - a formal determination by a qualified expert (§ 164.514(b)(1))
- Safe Harbor - the removal of specified individual identifiers as well as absence of actual knowledge by the covered entity that the remaining information could be used alone or in combination with other information to identify the individual (§ 164.514(b)(2))

Note that "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or medium, whether electronic, on paper, or oral are the ones protected by HIPAA rules and we call them as "protected health information". If such information was listed with health condition, health care provision or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI. For example, a medical record, laboratory report, or hospital bill would be PHI because each document would contain a patient's name and/or other identifying information associated with the health data content.

Either the covered entity themselves can de-identify PHI or they may use a Business Associate to de-identify PHI on its behalf only to the extent such activity is authorized by their business associate agreement.

18 HIPAA Identifiers	
Name	Email address
Address (all geographic subdivisions smaller than state, including street address, city county, and zip code)	All elements (except years) of dates related to an individual (including birthdate, admission date, discharge date, date of death, and exact age if over 89)
Telephone numbers	Fax Numbers
Social Security Number	Medical record number
Health plan beneficiary number	Account number
Certificate or license number	Vehicle identifiers and serial numbers, including license plate numbers;
Web URL	Internet Protocol (IP) Address
Finger or voice print	Photographic image - Photographic images are not limited to images of the face
Any other characteristic that could uniquely identify the individual	Device identifiers and serial numbers

UPCOMING

Top 4 HIPAA Initiatives for the month of May 2018

Train Intake Employees

The process of reducing the risk of HIPAA violations starts at your organization's front desk. Your receptionist or Intake employees must also be aware of HIPAA rules and how to implement them within their duties and daily tasks.

These personnel should know how they protect documents, PC's , facsimile and other means where PHI can be written or shown. Also, note that patient data cannot be given freely even within a practice; it must only be exchanged on a need to know basis. The RBAC system encompasses the role of the front desk personnel, they too must be given appropriate access depending on their roles within the organization.

HIPAA violations can be a big problem, but taking a few simple steps can be all it takes to put your organization on the right path.

For more HIPAA training videos
Subscribe to our YouTube Channel

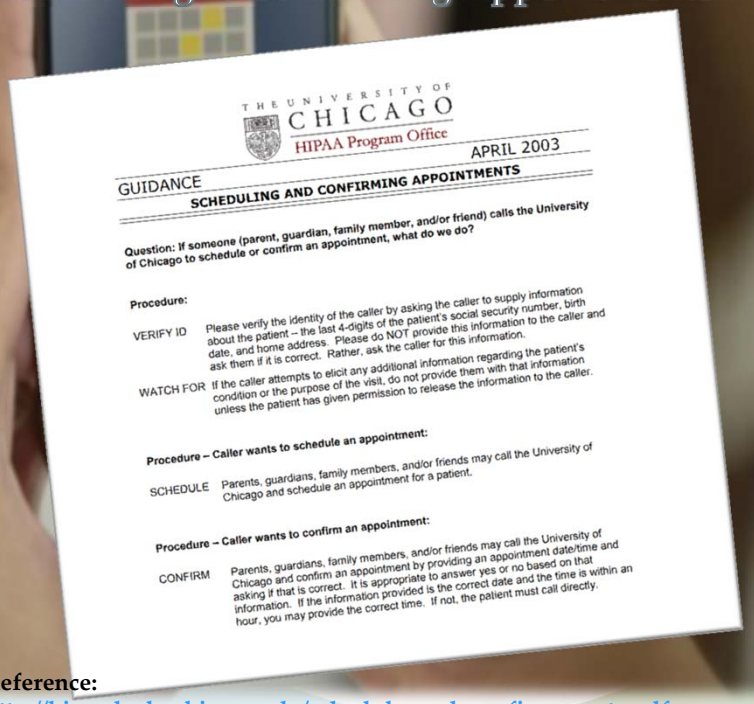
YouTube

COPY & PASTE ON YOUR BROWSER
https://www.youtube.com/channel/UCNr0MQ4B6qLBWMqQQPeXPww

Train People Who Confirm Appointments

Health and Human Services has approved of both the traditional postcard reminders and phone/email/text message reminders, as an integral part of patient care. Healthcare organization's appointment setters can send them in a form which is convenient to the patient (e.g. to their home email address rather than to their work email address, if requested, or to their cell phone instead of their home phone, if requested.) You should however minimize private health information in all appointment reminders, particularly with regards to health information which is especially sensitive. Do not include information about diagnoses or treatment plans in reminders. Other detailed information maybe given in person. These and more will be discussed comprehensively in HIPAA Awareness and Security Trainings therefore it is very important that your appointment setters undergo these trainings on a regular basis.

Sample Procedure For
Scheduling & Confirming Appointments



THE UNIVERSITY OF CHICAGO
HIPAA Program Office

GUIDANCE — APRIL 2003

SCHEDULING AND CONFIRMING APPOINTMENTS

Question: If someone (parent, guardian, family member, and/or friend) calls the University of Chicago to schedule or confirm an appointment, what do we do?

Procedure:

VERIFY ID — Please verify the identity of the caller by asking the caller to supply information about the patient -- the last 4-digits of the patient's social security number, birth date, and home address. Please do NOT provide this information to the caller and ask them if it is correct. Rather, ask the caller for this information.

WATCH FOR — If the caller attempts to elicit any additional information regarding the patient's condition or the purpose of the visit, do not provide them with that information unless the patient has given permission to release the information to the caller.

Procedure – Caller wants to schedule an appointment:

SCHEDULE — Parents, guardians, family members, and/or friends may call the University of Chicago and schedule an appointment for a patient.

Procedure – Caller wants to confirm an appointment:

CONFIRM — Parents, guardians, family members, and/or friends may call the University of Chicago and confirm an appointment by providing an appointment date/time and asking if that is correct. It is appropriate to answer yes or no based on that information. If the information provided is the correct date and the time is within an hour, you may provide the correct time. If not, the patient must call directly.

Reference:
http://hipaa.bsd.uchicago.edu/schedule_and_confirm_appts.pdf