A study on HIPAA compliance in health IT Company and its application to PHI

Academic year, 2016-2018

Guided by
Dr Anoop Khanna

By
Astha Billore
0398 (MBA HM 21)

IIHMR UNIVERSITY

Few words about the organisation…

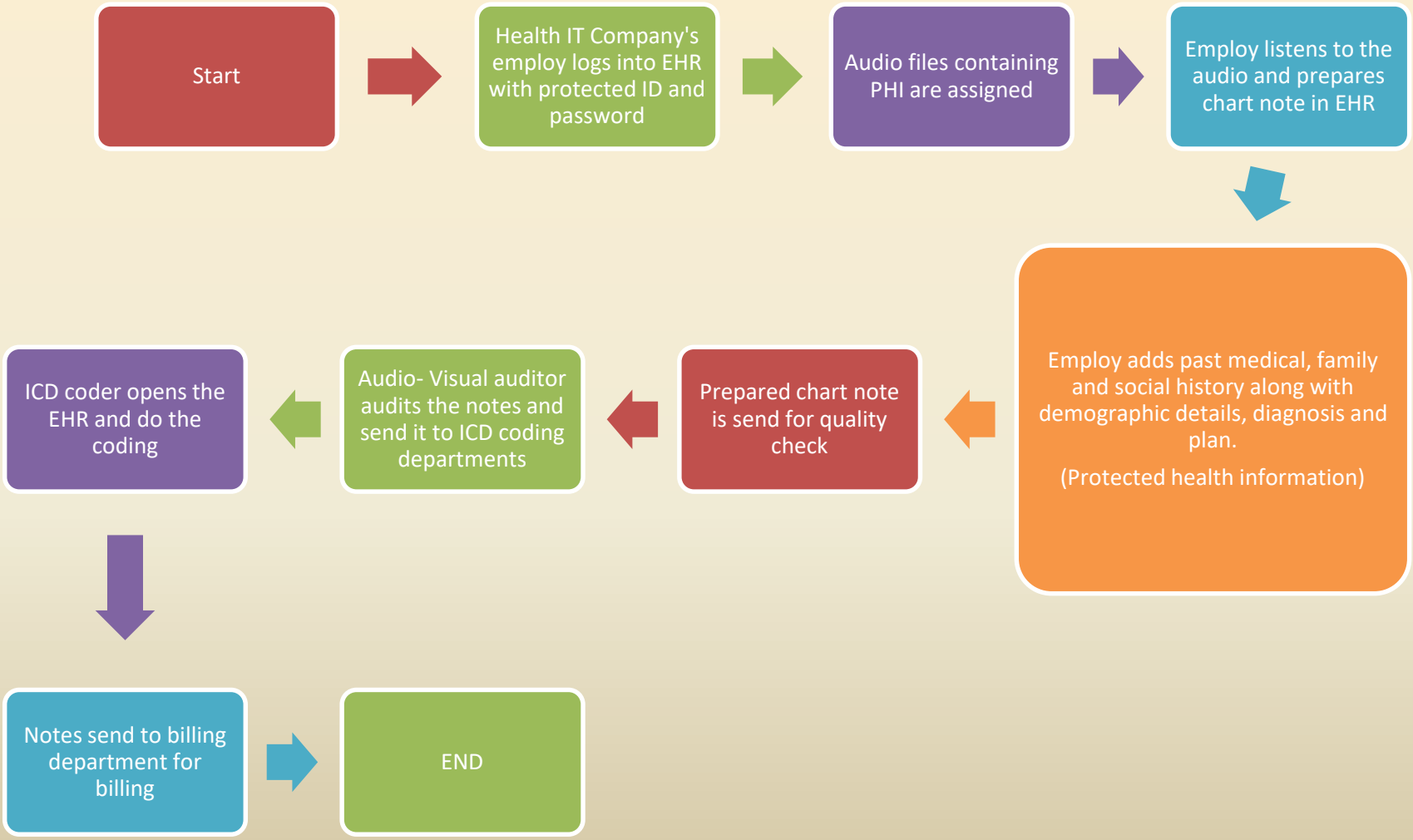
IKS HEALTH- Inventurus Knowledge Solutions

IKS Health is the premier partner for ambulatory care organizations nationwide. Bringing an integrated solutions set, coupled with insight into industry trends and direction, the team at IKS helps organizations perform more effectively for better clinical, financial, and organizational outcomes.

Three verticals of organisation are:

IKS CARE **IKS PRACTICE** **IKS MARGIN**

IKS CARE WORKFLOW



What is HIPAA compliance?

Prior to 1996, there was no legislation restricting the manner in which patient's healthcare related information was shared, distributed, store and protected.

On August 21, 1996 - HIPAA Passed by Congress Designed primarily to modernize health information exchange

The Health Insurance Portability and Accountability Act (**HIPAA**) set the standard for sensitive patient data protection. Companies that deal with protected health information (PHI) must have physical, network, and process security measures in place and follow them to ensure **HIPAA Compliance**.

HIPAA Timeline-Tracking Important Dates

August 21, 1996
HIPAA Passed by Congress Designed primarily to modernize health information exchange

2000-HIPAA Privacy Rule Finalized by HHs
Becomes the first federal healthcare information privacy law

2001-HIPAA Stalls
New Bush administration reopens HIPAA Privacy Rule comment period

2002-Bush Administration Announces Support of Modified HIPAA
Exceptions for "treatment, payment, and healthcare operations" added

2003
HIPAA Security Rule Finalized

April 14, 2003
HIPAA Privacy Rule Compliance Deadline

April 21, 2005
HIPAA Security Rule Compliance Deadline

2008-Lack of HIPAA Enforcement
More than 33,000 HIPAA complaints filed with OCR to date, only 8,000 investigated with no fines issued

February 17, 2009
ARRA's HITECH Act Signed into Law
HIPAA revised to strengthen enforcement penalties, require breach notifications, and expand patient rights

2009-OCR Ratchets up HIPAA Enforcement
Some entities fined millions of dollars for privacy breaches

January 25, 2013
HITECH's HIPAA Modification Final Rule Released

Three rules of HIPAA

HIPAA Privacy Rule

The HIPAA Privacy Rule sets national standards for patients' rights to PHI.

HIPAA Security Rule

The HIPAA Security Rule sets national standards for the secure maintenance, transmission, and handling of ePHI

HIPAA Breach Notification Rule

The HIPAA Breach Notification Rule is a set of standards that covered entities and business associates must follow in the event of a data breach containing PHI or ePHI.

Research aim and objectives

Research aim

The purpose of this study is to understand its application to HIPAA compliance in PHI.

Research objectives

- To understand PHI in Health IT company.
- To determine when HIPAA rules apply to PHI.
- To understand limiting release of PHI
- To determine ways to protect PHI
- To establish ways in order to keep workplace HIPAA compliant.
- To understand patient’s right in HIPAA compliance.

RESEARCH METHODOLOGY

- Type of study – Descriptive Cross sectional study
- Study Area- Health IT Company
- Duration of study- 4 weeks
- Primary data include- In-depth interview and consultations

Data interpretation

Significance of HIPAA

- The HIPAA Privacy Rule has helped to create a culture of compliance within many healthcare organizations. With the ever-changing environment of healthcare regulations, compliance is imperative.
- This privacy rule has also helped to build better security within organizations. To comply with the Act, security has had to improve both physically and electronically.
- When sharing patient files electronically, the HIPAA Privacy Rule has helped promote this ability between organizations. When a patient provides permission for sharing, many providers can send the records instantly through electronic means.
- The Act has even helped to develop national standards for healthcare information and patient confidentiality. In times past, there were few standards for how medical records were kept or secured.

Protected Health Information (PHI)

- Protected Health Information means any information, whether oral, written, recorded, in any form or medium that indicates or is related to an individual's past, present or future health status. This would include any physical or mental health condition, treatment or services provided.
- This information must be protected and generally can be used or disclosed only with the individual's permission.

Elements of PHI

- Patient's Name as well as name of the Insured
- Patient/Insured's Identification codes, Address, Telephone/Fax number or email-id
- Patient/Insured's Social Security Number (SSN)
- Employer's details and occupation
- Finger prints, Photographs or any other identification marks
- Medical history, treatment charts, X-Ray & other diagnostic reports
- Payment details – including Bank account numbers, check/electronic remittance details.
- Dates directly related to patient (except year), including DOB, admission or discharge date
- Telephone Number
- Driver's License Number
- Email addresses & FAX Numbers

Contd...

- Social Security Number
- Medical Record/Medical Record Number
- Health Plan Beneficiary Number
- Account Number
- Certificate/License Number
- Any vehicle or device serial number, including license plates
- Web Addresses (URLs)
- Internet Protocol (IP) Address
- Finger or voice prints
- Photographic images
- Any other unique identifying number, characteristic, or code
- Age greater than 89 (as the 90 year old and over population is relatively small)

When do HIPAA rules apply to PHI?

- When you use it
- When you disclose it
- When you store it
- When you see it on your computer
- When it is lying on your desk
- When you share it with another health care provider
- When you share it with another contracted service provider
- When you are talking about it face-to-face, in any public area
- When you are talking about it over the phone

"Texting my orders? No, I'm tweeting and updating my Facebook wall about this big Bozo I am treating."

PHI Violations

- **Access PHI to find out personal information about a patient, just out of curiosity**

- Example: While billing you come across a familiar name say a film actor so just out of curiosity you access patient information.

Access PHI of a patient not for work-related reasons

Example: Two colleagues from different processes discussing PHI of patient .

Access PHI of a friend or family member without having the appropriate authorization

Example: You come across name of a family friend and without his permission or knowledge you access his PHI

Recommendations

- PROPOSING STANDARD OPERATING PROCEDURES FOR HEALTH IT Company to be HIPAA COMPLIANT

- PROPOSING SELF-CHECK LIST FOR AN EMPLOY TO BE HIPPA COMPLIANT

PROPOSING STANDARD OPERATING PROCEDURES FOR HEALTH IT Company to be HIPAA COMPLIANT

Authorizations

- One must obtain written authorization is required for all uses and disclosures of PHI.

- Individual Authorization Is Required to Use Protected Health Information for:
  - Marketing
  - Initial Eligibility Enrollment
  - Disclosure to Employer for Employment Determinations
  - Treatment, Payment, and healthcare Operations (TPO)

Release of PHI

PHI can be released on the following situations:

- Release of PHI for Treatment.
- Example: Two providers can freely share PHI if they are both involved in the patient's care.
- Release of PHI for Payment.
- Example: A patient-accounts representative may release PHI to an insurance company as per requirement to obtain payment for services.
- PHI may be used to accomplish healthcare Operations.
- Example: Procedures must be followed to maintain an audit trail to monitor access and use.

Security & Confidentiality Agreement

All staff members are required to sign a Security and Confidentiality Agreement and protect the privacy of PHI obtained in the course of billing practices.

I, Astha Billore acknowledge that through my association with this company I may be able to view, send and/or receive protected health information (PHI), including without limitation patient-related claims information, and Medical Information for patients. In addition to my obligations in the Business Agreement regarding such information, I agree to maintain the security and privacy of such patient-related information, and agree that all such Information shall be held in strictest confidence.

I shall ensure that access to Patient Medical Information shall be limited to me on a "need to know" basis and that such information will be used solely for purposes relating to communications with Insurance Companies, Patients, and other such parties involved in health care operations. I also agree to promptly notify my department head in the event; I become aware of any violations of this provision.

PROPOSING SELF-CHECK LIST FOR AN EMPLOY TO BE HIPPA COMPLIANT

1. One User per Login Account

Logins cannot be shared. Sharing of login is a HIPAA violation.

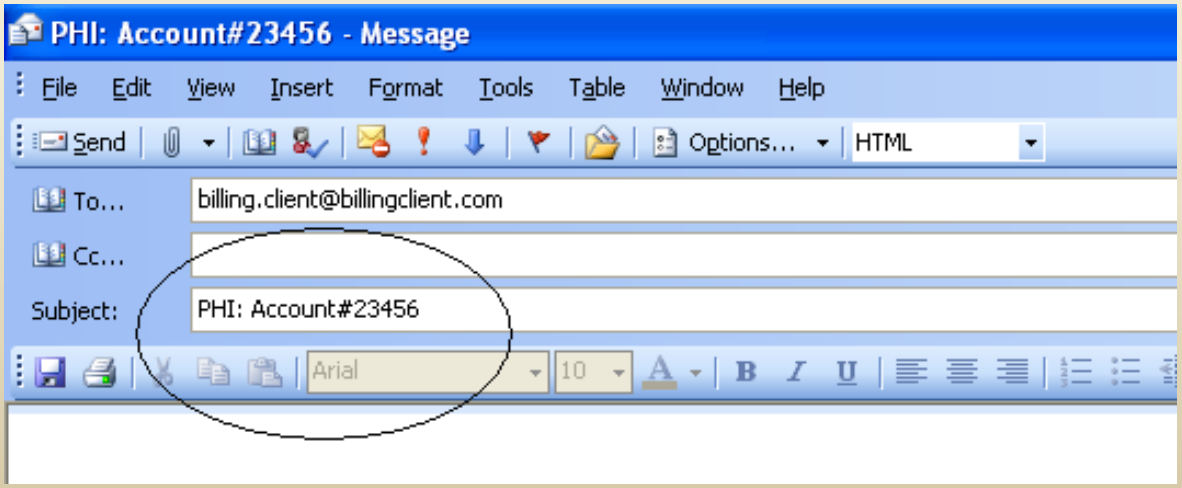
An individual is responsible for any activity that occurs under his/her login.

2.Use “PHI” in E - mail subject line

- Use “PHI” in the subject line of email to protect patient or other sensitive information.

  The subject line email is NOT protected so don’t use this area for sensitive information such as patient name and diagnosis.

  Password protected attachments are safe for PHI or other sensitive information.



3. Viruses and Worms

Do not open attachments and mails from unfamiliar/unknown sources.

Fire walls to be placed to prevent unauthorized access .

Do not install games or any other software.

4.Lock Computer Monitors, Electronic Displays

Turn electronic displays/monitors that contain PHI or other sensitive information away from public view

Log-off or lock your computer if you intend to leave it unattended for more than two minutes

5. Collect PHI's from printers

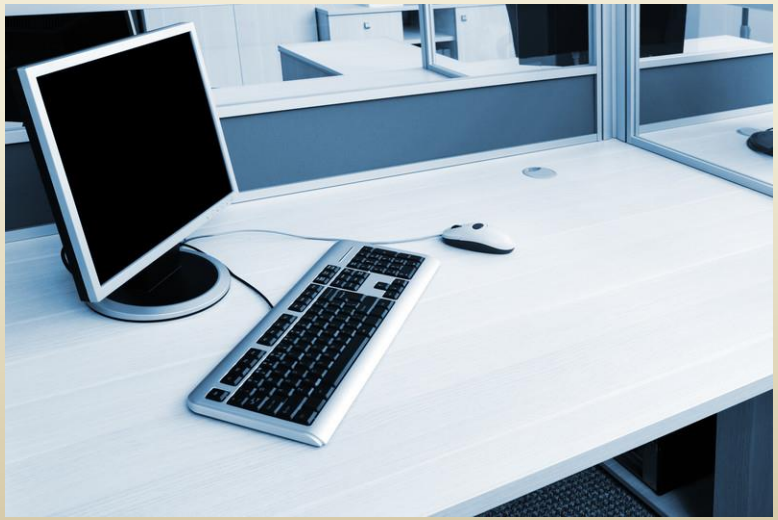
Never leave unattended PHI on printers. Collect all PHI that you have printed ASAP so that no one else has access to it.

6. Clean Desk policy

At the end of the working day clean working desk.

Do not leave any confidential data in any form as paper or CD unattended.

Always lock your PC while you are away from your desk.



Conclusion

All healthcare entities and organizations that use, store, maintain or transmit patient health information are expected to be in complete compliance with the regulations of the HIPAA law. When completely adhered to, HIPAA regulations not only ensure privacy, reduce fraudulent activity and improve data systems but are estimated to save providers billions of dollars annually. By knowing of and preventing security risks that could result in major compliance costs, organizations are able to focus on growing their profits instead of fearing these potential audit fines.


Thank You