Internship Training at

Deloitte Consulting India Pvt. Ltd.

By

Anshul Kapoor

PGDHM

2012-2014

IIHMR
DELHI

International Institute of Health Management Research

Internship Training

At

Deloitte Consulting US India Pvt. Ltd.

A study on EHR vendor and Deloitte's Compliance to the security and privacy rule under HIPAA

By

Anshul Kapoor

Under the guidance of

Dr. Abhijit Chakrabarty

Post Graduate Diploma in Hospital and Health Management

2012-2014

International Institute of Health Management Research

New Delhi

Deloitte.

Deloitte Consulting
India Pvt. Ltd.
2nd Floor, Salarpuria Supreme,
92/5, Munekolalu Village,
Varthur Hobli, Outer Ring Road,
Near Marthahalli Junction,
Bengaluru South 560 037, India.
Tel: +91 80 6755 1000
www.deloitte.com

May 02, 2014

To Whom It May Concern

This is to certify that Ms. **Anshul Kapoor** was on a fixed term Internship from **February 10, 2014** to **May 02, 2014**. She has successfully completed her Internship in **Application Management Services**.

We wish you the very best in your future endeavors.

Yours truly,

For Deloitte Consulting India Pvt. Ltd.

GUNJAN MITTAL

Digitally signed by GUNJAN MITTAL
DN: c=IN, o=Personal, ou=CID - 2677500, postalCode=500019, st=Andhra Pradesh, serialNumber=6e5ec5e5b1437ab538c76bd3dda7880b456ecc3b562d2f75d30ebb19b097e63d, cn=GUNJAN MITTAL
Date: 2014.05.02 18:14:51 +05'30'

Authorized Signatory

Certificate of Approval

The following dissertation titled **"To analyze software vendor and Deloitte's compliance to the security and privacy rule under HIPAA"** at **Deloitte Consulting US India Pvt. Ltd.** is hereby approved as a certified study in management carried out and presented in a manner satisfactorily to warrant its acceptance as a prerequisite for the award of **Post- Graduate Diploma in Health and Hospital Management** for which it has been submitted. It is understood that by this approval the undersigned do not necessarily endorse or approve any statement made, opinion expressed or conclusion drawn therein but approve the dissertation only for the purpose it is submitted.

Dissertation Examination Committee for evaluation of dissertation.

Name	Signature
PARTHA DEY	
Anandhi Ramachandran	
ABHIJIT CHAKRABORTY	05/03/14

TO WHOM IT MAY CONCERN

This is to certify that **ANSHUL KAPOOR** student of Post Graduate Diploma in Hospital and

Health Management (PGDHM) from International Institute of Health Management

Research, New Delhi has undergone internship training at **DELOITTE CONSULTING** from **10.02.2014** to **2.05.2014**.

The Candidate has successfully carried out the study designated to her during internship

training and her approach to the study has been sincere, scientific and analytical.

The Internship is in fulfillment of the course requirements.

I wish him all success in all his future endeavors.

05/05/2014

Dean, Academics and Student Affairs
IIHMR, New Delhi

Professor
IIHMR, New Delhi

FEEDBACK FORM

Name of the Student: ANSHUL KAPOOR

Dissertation Organisation: DELOITTE

Area of Dissertation: To analyse deloittes and the EHR Vendor's compliance to the privacy and security rule under the Health Insurance Portability and Accountability Act

Attendance: 98%

Objectives achieved: Anshul has met all the objectives set up by Deloitte

Deliverables: shadowed the Clin DOC team of Dt Incident and change managet

Strengths:

- Takes initiatives and is Proactive
- Articulates well
-

Suggestions for Improvement:

- Need to work on her listening skills

Signature of the Officer-in-Charge/Organisation Mentor (Dissertation)

Date: 30th April 14
Place: Bangalore

INTERNATIONAL INSTITUTE OF HEALTH MANAGEMENT RESEARCH, NEW DELHI

CERTIFICATE BY SCHOLAR

This is to certify that the dissertation titled **Analysis of EHR and Deloitte's compliance to the security and privacy rule under HIPAA** and submitted by **Anshul Kapoor**Enrollment No. **PG/012/013**under the supervision of **Dr. Abhijit Chakrabarty**for award of Postgraduate Diploma in Hospital and Health Management of the Institute carried out during the period from **10/2/2014 to 2/5/2014**embodies my original work and has not formed the basis for the award of any degree, diploma associate ship, fellowship, titles in this or any other Institute or other similar institution of higher learning.

Anshul Kapoor

Signature

ACKNOWLEDGEMENT

An internship is a golden opportunity for learning and self-development. I consider myself very lucky and honored to have so many wonderful people lead me through in completion of this project.

It is my glowing feeling to place on record my best regards, deepest sense of gratitude to Mr. Phani Kumar, Senior Manager for his judicious and precious guidance, which was extremely valuable for my study both theoretically and practically.

I wish to express my indebted gratitude and special thanks to Ms. Parerna Vashisht, Consultant, Deloitte who in spite of being extraordinarily busy with her duties, took time out to hear, guide and keep me on the correct path. I also thank Ms. Judith Monteiro and Mr. Tanvir Alam, who were a great support throughout the project

I express my deepest thanks to Mr. Abhiram Ravindrababu, Mr. Avinash Prasad and Mr. Ujjal das for taking part in useful decision & giving necessary advices and guidance and arranged all facilities to make life easier. I choose this moment to acknowledge their contribution gratefully.

I express my deepest thanks to Dr. Abhijit Chakrabarty, Assistant Professor, IIHMR, New Delhi for his guidance and support. He contributed his knowledge and experience to make this project a hit. He was there for me every time I had difficulties and I greatly appreciate the useful suggestions provided by him.

Anshul Kapoor

TABLE OF CONTENTS

List of Tables

List of Abbreviations

PHI	Protected Health Information
HIPAA	Health Insurance Portability and Accountability Act
EHR	Electronic Health Record
CE	Covered Entities
HMO	Health Maintenance Organization
PPO	Preferred Provider Organization
BA	Business Associates
HHS	Health and Human Services
OCR	Office of Civil rights
DBMS	Database Management System
LDAP	Light Directory Access Protocol
SSL	Secure Socket Layer
VPN	Virtual Private Network
GUI	Graphical User Interface
SOP	Statement of Purpose
MPLC	Multi-Protocol Label Switching
ODC	Offshore Delivery Center

1. INTRODUCTION

Protected health information (PHI) is any information about health status, provision of health care, or payment for health care that can be linked to a specific individual.

HIPAA (Health Insurance Portability and Accountability Act) regulations define health information as "any information, whether oral or recorded in any form or medium" that is “created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse"; and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual [1]."

In order to protect the privacy and confidentiality of this data the **Health Insurance Portability and Accountability Act** was enacted by the United States Congress and signed by President Bill Clinton in 1996 [2]. HIPAA encompasses of many parts, Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. The administrative simplification provisions also address the security and privacy of health data. The standards are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in the U.S. health care system.

As being a covered entity under this act, both Deloitte and the EHR vendor must comply with the set guidelines. This project aims to judge the level of compliance of Deloitte and the EMR to the Privacy and security rule under the title II of HIPAA and also suggest measures through which further improvement can take place.

2.REVIEW OF LITERATURE

ABOUT HIPAA

HIPAA is the Health Insurance Portability and Accountability Act of 1996 and is also known as Public Law 104-191 and the Kennedy-Kassebaum Bill, named after its creators, Senators Edward Kennedy and Kassebaum. This legislation was passed by the Congress, signed into law by Bill Clinton, and became effective on August 21, 1996 [3].

The overall goal of HIPAA is to provide insurance portability, fraud enforcement, and administrative simplification for the healthcare industry.

HIPAA was formed out of the growing concerns about keeping healthcare information private, the need to consolidate nonstandard healthcare data and transaction formats, as well as the general consensus to streamline healthcare operations and reduce the cost of providing healthcare services.

HIPAA holds five titles under it:

Title 1: HIPAA Health Insurance Reform

Title I of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) protects health insurance coverage for workers and their families when they change or lose their jobs.

Title II: HIPAA Administrative Simplification

The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) require the Department of Health and Human Services to establish national standards for electronic health care transactions and national identifiers for providers, health plans, and employers. It also addresses the security and privacy of health data. Adopting these standards will improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in health care.

There are four administrative simplification sub-sections, or rules, which include mandates for the privacy and security of personal and confidential healthcare information, referred to as the Privacy rule and Security Rule; standardized electronic transactions and code sets, referred to as the Electronic transactions and code Sets Rule; and national identifiers, referred to as the Unique Identifier Rules.

Title III: HIPAA Tax Related Health Provisions

Title III provides for certain deductions for medical insurance, and makes other changes to health insurance law.

Title IV: Application and Enforcement of Group Health Plan Requirements

Title IV specifies conditions for group health plans regarding coverage of persons with pre-existing conditions, and modifies continuation of coverage requirements.

Title V: Revenue Offsets

Title V includes provisions related to company-owned life insurance, treatment of individuals who lose U.S. Citizenship for income tax purposes and repeals the financial institution rule to interest allocation rules.

What HIPAA covers?

In addition to the various transactions and code set statements, HIPAA mandates protection of various forms of confidential health information referred to as Protected Health Information (PHI). PHI is considered and oral or recorded information relating to any past, present or future physical or mental health of an individual, provision of healthcare to the individual, or the payment for the healthcare of that individual.

Organizations that must comply with HIPAA

Covered Entities (CE)

Virtually the entire healthcare industry, as well as significant number of organizations in other industries, is affected by HIPAA in one way or another.

Large insurance companies to hospitals to self- insured employers to small physician practices are required to comply with HIPAA. These organisations are called Covered entity (CE). There are three main categories of CEs

i. Providers
ii. Health Plans: Individuals or group plans that provide or pay for medical care. Examples include HMOs, PPOs etc.
iii. Healthcare Clearinghouse: These are public or private entities that process or facilitate the processing of nonstandard data elements of health information into a standard format for electronic transactions. Example includes billing services etc.

Business Associates

Individuals or organizations doing business with CEs, referred to as business associates (BAs), may be affected by HIPAA as well. In order to fall into the business associate category, these individuals or organizations must perform an activity involving the use or disclosure of PHI on behalf of a CE. This does not include performing any activities as an employee of the CE.

For any BA relationship that CE has, a BA agreement that holds the BAs responsible for certain HIPAA requirements must be in place between the two parties.

HIPAA Penalties and enforcements

Like other laws affecting the healthcare industry such as OSHA, HIPAA must be taken seriously. There are “slap on the hand” civil penalties that start at $100 per incident, as well as severe criminal penalties that include huge fines and possible prison time [4].

For non-criminal violation of the HIPAA rules, including disclosures made in error, civil penalties of $100 per violation up to 425000 per year, per standard, may be issued. Additionally, criminal penalties may be applied for certain violations done knowingly as follows:

- *Wrongful disclosure offense*: 450,000 fine, no more than 1 year in prison, or both
- *Offense under false pretenses*: $100,000 fine, no more than 5 years in prison, or both
- *Offence committed with intent to sell information*: $250,000 fine, no more than 10 years in prison, or both [5].

THE PRIVACY RULE

The Standards for Privacy of Individually Identifiable Health Information (“Privacy Rule”) establishes, for the first time, a set of national standards for the protection of certain health information. The U.S. Department of Health and Human Services (“HHS”) issued the Privacy Rule to implement the requirement of HIPAA. [6] The Privacy Rule standards address the use and disclosure of PHI by organizations subject to the Privacy Rule — called “covered entities,” as well as standards for individuals' privacy rights to understand and control how their health information is used. Within HHS, the Office for Civil Rights (“OCR”) has responsibility for implementing and enforcing the Privacy Rule with respect to voluntary compliance activities and civil money penalties [7].

A major goal of the Privacy Rule is to assure that individuals’ health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and wellbeing. The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing. Given that the health care marketplace is diverse, the Rule is designed to be flexible and comprehensive to cover the variety of uses and disclosures that need to be addressed

General Principle for Uses and Disclosures

Basic Principle: A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual’s protected heath information may be used or disclosed by covered entities. A covered entity may not use or disclose protected health information, except either:

(1) The Privacy Rule permits or requires; or

(2) The individual who is the subject of the information (or the individual’s personal representative) authorizes in writing. [8]

Required Disclosures: A covered entity must disclose protected health information in only two situations: (a) to individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their protected health information; and (b) to HHS when it is undertaking a compliance investigation or review or enforcement action [9].

Permitted Uses and Disclosures

A covered entity is permitted, but not required, to use and disclose protected health information, without an individual's authorization, for the following purposes or situations:

(1) To the Individual (unless required for access or accounting of disclosures);

(2) Treatment, Payment, and Health Care Operations;

(3) Opportunity to Agree or Object;

(4) Incident to an otherwise permitted use and disclosure;

(5) Public Interest and Benefit Activities; and (6) Limited Data Set for the purposes of research, public health or health care operations.18 Covered entities may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make. [10]

Limiting Uses and Disclosures to the Minimum Necessary

Minimum Necessary: A central aspect of the Privacy Rule is the principle of "minimum necessary" use and disclosure. A covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request. [11] A covered entity must develop and implement policies and procedures to reasonably limit uses and disclosures to the minimum necessary. When the minimum necessary standard applies to a use or disclosure, a covered entity may not use, disclose, or request the entire medical record for a particular purpose, unless it can specifically justify the whole record as the amount reasonably needed for the purpose.

The minimum necessary requirement is not imposed in any of the following circumstances: (a) disclosure to or a request by a health care provider for treatment; (b) disclosure to an individual who is the subject of the information, or the individual's personal representative; (c) use or disclosure made pursuant to an authorization; (d) disclosure to HHS for complaint investigation, compliance review or enforcement; (e) use or disclosure that is required by law; or (f) use or disclosure required for compliance with the HIPAA Transactions Rule or other HIPAA Administrative Simplification Rules. [12]

Access and Uses.

For internal uses, a covered entity must develop and implement policies and procedures that restrict access and uses of protected health information based on the specific roles of the members of their workforce. These policies and procedures must identify the persons, or classes of persons, in the workforce who need access to protected health information to carry out their duties, the categories of OCR Privacy Rule Summary 11 Last Revised 05/03 protected health information to which access is needed, and any conditions under which they need the information to do their jobs.

- Disclosures and Requests for Disclosures: Covered entities must establish and implement policies and procedures (which may be standard protocols) for routine, recurring disclosures, or requests for disclosures, that limits the protected health information disclosed to that which is the minimum amount reasonably necessary to achieve the purpose of the disclosure. Individual review of each disclosure is not required. For non-routine, non-recurring disclosures, or requests for disclosures that it makes, covered entities must develop criteria designed to limit disclosures to the information reasonably necessary to accomplish the purpose of the disclosure and review each of these requests individually in accordance with the established criteria.
- Reasonable Reliance: If another covered entity makes a request for protected health information, a covered entity may rely, if reasonable under the circumstances, on the request as complying with this minimum necessary standard. Similarly, a covered entity may rely upon requests as being the minimum necessary protected health information from: (a) a public official, (b) a professional (such as an attorney or accountant) who is the covered entity’s business associate, seeking the information to provide services to or for the covered entity; or (c) a researcher who provides the documentation or representation required by the Privacy Rule for research.[12]

Administrative Requirements

HHS recognizes that covered entities range from the smallest provider to the largest, multi-state health plan. Therefore the flexibility and scalability of the Rule are intended to allow covered entities to analyze their own needs and implement solutions appropriate for their own environment. What is appropriate for a particular covered entity will depend on the nature of the covered entity's business, as well as the covered entity's size and resources.

i. Privacy Policies and Procedures: A covered entity must develop and implement written privacy policies and procedures that are consistent with the Privacy Rule. [13]

ii. Privacy Personnel: A covered entity must designate a privacy official responsible for developing and implementing its privacy policies and procedures, and a contact person or contact office responsible for receiving complaints and providing individuals with information on the covered entity's privacy practices. [14]

iii. Workforce Training and Management: Workforce members include employees, volunteers, trainees, and may also include other persons whose conduct is under the direct control of the entity (whether or not they are paid by the entity).66 A covered entity must train all workforce members on its privacy policies and procedures, as necessary and appropriate for them to carry out their functions. [15] A covered entity must have and apply appropriate sanctions against workforce members who violate its privacy policies and procedures or the Privacy Rule. [16]

iv. Mitigation: A covered entity must mitigate, to the extent practicable, any harmful effect it learns was caused by use or disclosure of protected health information by its workforce or its business associates in violation of its privacy policies and procedures or the Privacy Rule. [17]

v. Data Safeguards: A covered entity must maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information in violation of the Privacy Rule and to limit its incidental use and disclosure pursuant to otherwise permitted or required use or disclosure. [18] For example, such safeguards might include shredding documents containing protected health information before discarding them, securing medical records with lock and key or pass code and limiting access to keys or pass codes.

vi. Complaints: A covered entity must have procedures for individuals to complain about its compliance with its privacy policies and procedures and the Privacy Rule. [19] The covered entity must explain those procedures in its privacy practices notice.

vii. Among other things, the covered entity must identify to whom individuals can submit complaints to at the covered entity and advise that complaints also can be submitted to the Secretary of HHS.

viii. Retaliation and Waiver: A covered entity may not retaliate against a person for exercising rights provided by the Privacy Rule, for assisting in an investigation by HHS or another appropriate authority, or for opposing an act or practice that the person believes in good faith violates the Privacy Rule.

ix. Documentation and Record Retention: A covered entity must maintain, until six years after the later of the date of their creation or last effective date, its privacy policies and procedures, its privacy practices notices, disposition of complaints, and other actions, activities, and designations that the Privacy Rule requires to be documented. [20]

THE SECURITY RULE

The Security Standards for the Protection of Electronic Protected Health Information (the Security Rule) establish a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called “covered entities” must put in place to secure individuals’ “electronic protected health information” (e-PHI). Within HHS, the Office for Civil Rights (OCR) has responsibility for enforcing the Privacy and Security Rules with voluntary compliance activities and civil money penalties.

Prior to HIPAA, no generally accepted set of security standards or general requirements for protecting health information existed in the health care industry. At the same time, new technologies were evolving, and the health care industry began to move away from paper processes and rely more heavily on the use of electronic information systems to pay claims, answer eligibility questions, provide health information and conduct a host of other administrative and clinically based functions.

Today, providers are using clinical applications such as computerized physician order entry (CPOE) systems, electronic health records (EHR), and radiology, pharmacy, and laboratory systems. Health plans are providing access to claims and care management, as well as member self-service applications. While this means that the medical workforce can be more mobile and efficient (i.e., physicians can check patient records and test results from wherever they are), the rise in the adoption rate of these technologies increases the potential security risks.

A major goal of the Security Rule is to protect the privacy of individuals' health information while allowing covered entities to adopt new technologies to improve the quality and efficiency of patient care. Given that the health care marketplace is diverse, the Security Rule is designed to be flexible and scalable so a covered entity can implement policies, procedures, and technologies that are appropriate for the entity's particular size, organizational structure, and risks to consumers' e-PHI.

General Rules

The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI.

Specifically, covered entities must:

- Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
- Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- Protect against reasonably anticipated, impermissible uses or disclosures; and
- Ensure compliance by their workforce. [21]

The Security Rule defines "confidentiality" to mean that e-PHI is not available or disclosed to unauthorized persons. The Security Rule's confidentiality requirements support the Privacy Rule's prohibitions against improper uses and disclosures of PHI. The Security rule also promotes the two additional goals of maintaining the integrity and availability of e-PHI. Under the Security Rule, "integrity" means that e-PHI is not altered or destroyed in an unauthorized manner. "Availability" means that e-PHI is accessible and usable on demand by an authorized person.

HHS recognizes that covered entities range from the smallest provider to the largest, multi-state health plan. Therefore the Security Rule is flexible and scalable to allow covered entities to analyze their own needs and implement solutions appropriate for their specific environments. What is appropriate for a particular covered entity will depend on the nature of the covered entity's business, as well as the covered entity's size and resources.

Therefore, when a covered entity is deciding which security measures to use, the Rule does not dictate those measures but requires the covered entity to consider:

- Its size, complexity, and capabilities,
- Its technical, hardware, and software infrastructure,
- The costs of security measures, and
- The likelihood and possible impact of potential risks to e-PHI.[22]

Covered entities must review and modify their security measures to continue protecting e-PHI in a changing environment.

Administrative Safeguards

i. Security Management Process: As explained in the previous section, a covered entity must identify and analyze potential risks to e-PHI, and it must implement security measures that reduce risks and vulnerabilities to a reasonable and appropriate level.

ii. Security Personnel: A covered entity must designate a security official who is responsible for developing and implementing its security policies and procedures. [23]

iii. Information Access Management: Consistent with the Privacy Rule standard limiting uses and disclosures of PHI to the "minimum necessary," the Security Rule requires a covered entity to implement policies and procedures for authorizing access to e-PHI only when such access is appropriate based on the user or recipient's role (role-based access). [24]

iv. Workforce Training and Management: A covered entity must provide for appropriate authorization and supervision of workforce members who work with e-PHI.17 A covered entity must train all workforce members regarding its security policies and procedures,18 and must have and apply appropriate sanctions against workforce members who violate its policies and procedures. [25]

v. Evaluation: A covered entity must perform a periodic assessment of how well its security policies and procedures meet the requirements of the Security Rule. [25]

Physical Safeguards

i. Facility Access and Control: A covered entity must limit physical access to its facilities while ensuring that authorized access is allowed. [26]

ii. Workstation and Device Security: A covered entity must implement policies and procedures to specify proper use of and access to workstations and electronic media. A covered entity also must have in place policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of electronic protected health information (e-PHI). [27]

Technical Safeguards

i. Access Control: A covered entity must implement technical policies and procedures that allow only authorized persons to access electronic protected health information (e-PHI). [28]

ii. Audit Controls: A covered entity must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI. [29]

iii. Integrity Controls: A covered entity must implement policies and procedures to ensure that e-PHI is not improperly altered or destroyed. Electronic measures must be put in place to confirm that e-PHI has not been improperly altered or destroyed. [30]

iv. Transmission Security: A covered entity must implement technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic network.

Required and Addressable Implementation Specifications

Covered entities are required to comply with every Security Rule "Standard." However, the Security Rule categorizes certain implementation specifications within those standards as "addressable," while others are "required." The "required" implementation specifications must be implemented. The "addressable" designation does not mean that an implementation specification is optional. However, it permits covered entities to determine whether the addressable implementation specification is reasonable and appropriate for that covered entity. If it is not, the

Security Rule allows the covered entity to adopt an alternative measure that achieves the purpose of the standard, if the alternative measure is reasonable and appropriate. [31]

Organizational Requirements

Covered Entity Responsibilities: If a covered entity knows of an activity or practice of the business associate that constitutes a material breach or violation of the business associate's obligation, the covered entity must take reasonable steps to cure the breach or end the violation. Violations include the failure to implement safeguards that reasonably and appropriately protect e-PHI.

Business Associate Contracts: HHS is developing regulations relating to business associate obligations and business associate contracts under the HITECH Act of 2009.

Policies and Procedures and Documentation Requirements

A covered entity must adopt reasonable and appropriate policies and procedures to comply with the provisions of the Security Rule. A covered entity must maintain, until six years after the later of the date of their creation or last effective date, written security policies and procedures and written records of required actions, activities or assessments.30 A covered entity must periodically review and update its documentation in response to environmental or organizational changes that affect the security of electronic protected health information (e-PHI). [32]

3. OBJECTIVE

To analyze Deloitte’s and the EHR Vendor’s compliance to the privacy and security rule under the Health Insurance Portability and Accountability Act (HIPAA) and further recommend measures of improvement.

4. METHODOLOGY

Descriptive study was conducted using secondary data such as documents provided by the firm such as Deloitte’s runbook, contracts etc. also many documents from the EMR vendor’s site were consulted.

None of the documents can be presented or attached with this study as it would result in a breach.

5. RESULTS

The EHR Vendor has made tedious efforts to be compliant to both the HIPAA Privacy rule and the Security Rule;

PRIVACY RULE

Business Associate Agreements

From time to time during the implementation and after the go live, the EHR Vendor personnel that are working with the organization might need to view protected health information of patients in the system. As a result, vendor may be considered a “business associate” under the rules, which may require organization to enter into a business associate agreement with vendors relating to vendor’s use and disclosure of protected health information. Vendor executes appropriate business associate agreements as necessary to satisfy these requirements.

Acknowledgement of Privacy Practices and Authorizations for Disclosure

Vendor’s patient database includes tables where users can record multiple consent or acknowledgement documents for each patient, including the document’s status (for example, received or withdrawn) and effective dates. Vendor also allows users to record patient notices, including directives to be omitted from hospital directories or solicitations.

The August 2002 revisions to the rule changed the consent requirements outlined in the original rule. Direct providers are required to document a good faith effort to obtain an acknowledgement of receipt of privacy policies. To comply with this, EHR vendor recommended that the organization use the system documents table.

EMR also provides means to alert users at the start of a patient encounter of a patient’s status with respect to a specific document, such as an acknowledgement of privacy practices. For example, you can set up the patient header to show the privacy acknowledgement status.

Vendor’s electronic medical record, EMRCare, can store patient authorizations as discrete encounter types. This information is reportable, which means that an organization can identify patients for whom users haven’t collected consents and authorizations. With the EMRCare letter writing module, organizations can create and distribute consents, authorizations, notices of privacy practices, and other patient communications regarding protected information.

“Minimum Necessary” Requirement

Vendor software helps organizations comply with the “minimum necessary” disclosure requirement by excluding certain “sensitive” encounters (for example, psychiatric visits) and orders (for example, HIV tests) from responses to disclosure requests. Only the authorizing provider, his supervisor, and designated proxies can view encounters and orders designated as sensitive. EHR’s role-based and context-based access controls also assist in this area.

De-Identifying Protected Health Information

With vendor’s Clarity Enterprise Reporting system, administrators can block identifying information from unauthorized users. To allow this, the system encrypts the IDs that are used for linking tables and by prevents the extraction of identifying information into the Clarity tables that are available to most users. [33] As an alternative to blocking the extraction of identifying information, administrators can use restrictive database views within the Clarity DBMS to control access to patient identifying information. These techniques can be used together to protect patient privacy while increasing the utility of your reporting platform.

Additionally, as of the 2007 version, EHR software includes a Data Scrambler utility that removes and replaces identifiable confidential data for testing, training, and demonstration environments.

Accounting of Disclosures

With vendor's Release of Information module, organizations record releases and disclosures, and capture the required information, including what was sent, to whom it was sent, the date it was sent, and the reason for the release. The Release of Information module can also be used to track and scan patient authorizations for releases. Organizations run the Patient Disclosure Report to generate an accounting of disclosures for a specific patient.

Monitoring Compliance

Vendor software's standard audit trails monitor access at the user, content and functional levels by capturing the user ID, date and instant of access, module accessed, and operation performed (for example, accepted or canceled). Supervisors can examine audit trail information and track accesses to personal health information with vendor's reporting tools.

SECURITY RULE

Table 1. EMR Security Functional Summary

Requirement	**Implementation Specification**	**EMR Feature**
Access Control	Unique user identification (Required)	Unique user records Security classes and user roles
	Emergency access (Required)	Break-the-Glass
	Automatic logoff (Addressable)	Automatic time-out settings
	Encryption and decryption (Addressable)	SSL, VPN Encryption of data on handheld devices Encryption of data at rest
Audit Controls	Audit controls (Required)	Audit trails Access logging

		Edit trails Security policy checks (Break-the-Glass)
Integrity	Mechanism to authenticate electronic protected health information (Addressable)	Audit trails Edit trails Journals
Person or Entry Authentication	Person or entity authentication (Required)	Unique user ID Password rules Integration with directory services via LDAP Biometrics Token and other two-factor devices
Transmission Security	Integrity controls (Addressable)	State of the art internet protocol
	Encryption (Addressable)	SSL, VPN compatibility

Vendor's software offers a multi-layered security architecture that includes record access controls, an emergency access option, multiple authentication capabilities, and an automatic logout feature. Vendor's clinical applications protect encounter records from alterations by preventing users from changing encounters once they are closed.

Authentication Controls

All of the applications make use of the same set of unique user records. Users have to enter their unique IDs and passwords to log in to EMR, and it can require users to re-authenticate their identities by providing their passwords at key points in the workflow. One can define password rules to enforce password expiration, complexity requirements, and re-use restrictions.

The graphical User Interface (GUI) of EMR is also used with biometric mechanisms such as fingerprint readers, or token systems such as Secure ID cards. The GUI authentication module is an extensible component, which allows for the use of virtually any two-factor or strong authentication mechanism. Additionally, the user interface can cooperate in cross-vendor single sign-on and authorization systems.

Audit Trails for System Access and Activity

Audit trails in the software enables to monitor access at the user, content, and functional levels by capturing the user ID, date and instant of access, module accessed, and operation performed.

For logging changes to data in system settings, EHR offers Item and Record Auditing. Item Auditing is used to keep track of the history of items changed over all editing sessions, including previous values. Record Auditing tracks creations, deletions, ID changes; name changes, and merges for master files.

EMR reporting tools are used to examine audit trail information. Also, the web-based MyChart application can be configured to allow patients to see who accessed their record and when, through the "Who Accessed My Record" feature.

Encryption of Data at Rest

Oracle 10G/11G and SQL Server, which are options for the Clarity analytical reporting database, offer Transparent Data Encryption (TDE). TDE uses multiple encryption keys to encrypt the data in the database.

In addition to these options for encrypting data at rest, multi-layered security structure of the software protects data while it is in the system. All data is stored in the database or the BLOB (Binary Large Object) server, which are both assumed to reside within the client hardened data center and are subject to the same physical and network security as existing systems.

Protections for remote access and data transmission

The software is compatible with tools that help protect against unauthorized remote access and support secure electronic transmission of data. Applications running in Graphical user interface (GUI) function in a layered communication environment, allowing the client to use industry-standard transmission protections as necessary. The EMR supports remote user access via a third-party Virtual Private Network (VPN) solution to create a secure tunnel to the system.

Vendor's handheld applications protect patient identifiable information both in transit and at rest. When data sent to the device during sync or wireless access, 128-Bit Secure Socket Layer (SSL) is used. When data is stored on the device, it is encrypted with AES-128, in addition to AES-256 hardware-level encryption available on newer Apple devices. The interconnect communications platform for interfacing with external systems via a variety of messaging standards may be secured with SSL encryption.

Access controls and emergency access

A user’s unique ID is associated with one or more security classifications and a user role. Security classifications contain security points, which control access to various modules and limit who can perform specific tasks such as ordering procedures or medications. Security classifications control access to functions and types of data. Context-based and emergency-based access is reflected in the security policy checks component of the Break-the-Glass feature.

Additionally, the web-based EMRCare Link and PlanLink applications provide organization’s affiliates with time-limited managed access to a limited set of patient records, as well as auditable necessity-based access via its First Access feature.

Data Backup, Emergency Operations, Disaster Recovery

EMR recommends a backup strategy that uses operating system or enterprise backup utilities. In addition to regularly scheduled backups, vendor requires redundant data disks. With this configuration, the database server continues operating in the event of disk failure.

In the event that both the production and failover servers fail, or in the event that production data becomes unavailable, EMR provides several options for downtime accessibility. With the first, users access a read-only EMR environment on a shadow server.

A separate option, Business Continuity Access (BCA) reporting, generates printed reports during an extended downtime when the vendor database cannot be accessed. These reports are generated on the reporting shadow server and then are stored on designated BCA PCs and/or a web server, depending on the organization’s configuration.

EMR provides for database logging and recovery with the method of journaling: A journaling file system is a file system that keeps track of the changes that will be made in a journal (usually a circular log in a dedicated area of the file system) before committing them to the main file system.

Efforts done by Deloitte to be compliant to the HIPAA Security Rule;

The following table shows the standards necessary to be compliant to the rule and also measures taken up by Deloitte to fulfill them.

Table 2. HIPAA Security Rule Checklist

HIPAA Security Rule Standard Implementation Specification	**Implementation**	**Requirement Description**	**Deloitte**
Security Management Process	Required	Policies and procedures to manage security violations	Written document, Statement of Purpose (SOP) documents all policies and procedures for the same.
Risk Analysis/ Risk Management	Required	Conduct vulnerability assessment	Deloitte Infrastructural setup (Firewall)
Sanction Policy	Required	Worker sanction for policies and procedures violations	Maintained by Deloitte as an entity (Applicable to compliant projects)
Assigned Security Responsibility	Required	Identify security official responsible for policies and procedures	Infrastructural Security Manager
Workforce Security	Required	Implement policies and procedures to ensure appropriate PHI access	Inbuilt tool to encrypt data, dedicated port (MPLS)
Authorization and/or Supervision	Addressable	Authorization/supervision for PHI access	Applicable to all analysts
Workforce Clearance Procedure	Addressable	Procedures to ensure appropriate PHI access	conducted by the Infrastructural Security Manager
Termination Procedures	Addressable	Procedures to terminate PHI access security policy document management	managed by the Client
Information Access	Required	Policies and procedures to authorize access to PHI	managed by client

Management			
Isolation Health Clearinghouse Functions	Required	Policies and procedures to separate PHI from other operations	MPLS
Access Authorization	Addressable	Policies and procedures to authorize access to PHI	By consensus between the client and Deloitte.
Security Awareness Training	Required	Training program for workers and managers	BOOTCAMP, Training on HIPAA, PHI, PII
Protection from Malicious Software	Addressable	Procedures to guard against malicious software host/network IPS, unified threat management, network anomaly detection, patch management, firmware management, host/network IDS, OS access controls (least-privileged user), content filtering	Deloitte Infrastructural and Networking Team
Password Management	Addressable	Procedures for password management	Frontend and Backend log in into the EHR is managed by the client
Security Incident Procedures	Required	Policies and procedures to manage security incidents	Documented Policies in the SOP
Response and Reporting	Required	Mitigate and document security incidents	In case of Breach, Deloitte reports to the Client
Contingency Plan	Required	Emergency response policies and procedures	Business Continuity Plan and Disaster Recovery Plan at the firm level
Data Backup Plan/ Emergency mode operation Plan	Required	Data backup planning and procedures	No data handheld by Deloitte, managed by Client
Disaster-Recovery Plan	Required	Data recovery planning and procedures	Offshore delivery centers at different locations across India
Evaluation	Required	Periodic security evaluation	Internal and external Audits
Business Associate written Contracts and Other Arrangements	Required	CE implement BACs to ensure safeguards	Written contract exits between the firm and client.

Facility Access Controls	Required	Policies and procedures to limit access to systems and facilities and also for personnel	ODC Policy and Procedures
Contingency Operations	Addressable	Procedures to support emergency operations and recovery	Biometrics, door beep after every 15 seconds if left open.
Facility Security Plan	Addressable	Policies and procedures to safeguard equipment and facilities	Clean Room setup
Maintenance Records	Addressable	Policies and procedures to document security-related repairs and modifications	Dedicated Security Helpdesk
Workstation Use	Required	Policies and procedures to specify workstation environment and use	No USB, no Screen Shots, no CDs, no Webcams allowed in the clean room.
Workstation Security	Required	Physical safeguards for workstation access	Locks, RSA Token
Device and Media Controls	Required	Policies and procedures to govern receipt and removal of hardware and media	Pen drives, CDs, Camera Phones, Personal Laptops not allowed in the clean room
Disposal/ Media Reuse	Required	Policies and procedures to manage media and equipment disposal and reuse	Restricted usage of media and equipment.
Access Control	Required	Technical (administrative) policies and procedures to manage PHI access	Clean Rooms, MPLS
Unique User Identification	Required	Assign unique IDs to support tracking	VPN (virtual private network) to use client network
Emergency Access Procedure	Required	Procedures to support emergency access	Required Managerial Approval
Encryption and Decryption/ Authenticate PHI	Addressable	Mechanism for encryption of PHI	#SECURE# Prefixed to encrypt data over an email.
Integrity	Required	Policies and procedures to safeguard PHI unauthorized alteration	No alterations Possible, restricted usage
Transmission Security	Required	Measures to guard against unauthorized access to	Dedicated MPLS Setup

		transmitted PHI	
Integrity Controls	Addressable	Measures to ensure integrity of PHI on transmission	VPN, Soft Token

MPLS (Multilevel protocol Label Switching)

It is a switching technology, which forwards packets in a network according to so called labels attached to the packets. These labels are attached as soon as the packet enters the MPLS core and are potentially modified as the packet transverses the network. The final label is removed as soon as the packet leaves the core [34]. There are number of advantages over traditional IP routing with this approach, regarding speed and security, as MPLS offers VPN functionality by traffic separation.

RSA Token

The RSA SecurID authentication mechanism consists of a "token" — either hardware (e.g. a USB dongle) or software (a soft token) — which is assigned to a computer user and which generates an authentication code at fixed intervals (usually 60 seconds) using a built-in clock and the card's factory-encoded random key (known as the "seed"). The seed is different for each token. On-Demand tokens are also available, which provide a token code via email or SMS delivery, eliminating the need to provision a token to the user.

VPN (Virtual Private Network)

A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it is directly connected to the private network, while benefiting from the functionality, security and management policies of the private network. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryptions.

6. CONCLUSION & DISCUSSION

As being a covered entity under HIPAA, the vendor has state of the art features to make sure patient data is protected. Features such as unique user identification, break the glass, data scramble etc. ensures privacy and security of PHI. If further revisions to or interpretations of the Security Rule are published, vendor would make all efforts to use the information to guide future development. In addition, vendor is a member of the Workgroup for Electronic Data Interchange (WEDI), which has been designated to play an important role in the standards setting process defined in the HIPAA legislation. WEDI also provides a Strategic National Implementation Process (SNIP) guide for HIPAA. Also, vendor's staff members regularly receive information from public policy groups and attend seminars regarding HIPAA issues. The development plans of the vendor are guided by HIPAA and Meaningful Use standards as they continue to emerge.

Deloitte bound by the business associate agreement has also incorporated almost all the measures so as to be compliant to the above discussed rule. The Clean room and ODC setup is well taken care of and routine audits both internal and external are conducted. Since the inception of the project, there has been no security breach from Deloitte's side and of course, it would make sure none happens in the future.

7. RECOMMENDATIONS

Though being almost perfect in every aspect of the Security and Privacy rule, there are a few recommendations that Deloitte can conform to in order to ensure cent percent compliance;

- Creating more awareness about PHI among the analysts by distributing regular security updates, sending monthly memos, email and fixing posters in the clean room or workstations depicting how important it is to protect PHI.
- Also, there must be periodic reinforcement of policies and procedures to make sure the HIPAA compliance is been met.

8. LIMITATIONS OF THE STUDY

- None of the documents consulted for conducting the study could be attached due to their confidentiality.
- Neither the name of the vendor or the client could be used throughout the study.

9. REFERENCES

[1] US department of Health and Human services, hhs.gov.

[2], [3], [4] US Government Printing Office, Full HIPAA Text. Pub.L. 104–191

[5] About Health Insurance Portability and accountability Act, Robert M. Callif et.al.

[6], [7], [8] HIPAA, a practical guide to security and privacy of data, June M. Sullivan, published in 2008.

[9] US department of Health and Human Services, privacy, HIPAA, Summary.

[10], [11], [12], [13] HIPAA, a practical guide to security and privacy of data, June M. Sullivan, published in 2008

[14], [15], [16] Federal Register, the daily journal of US government, HIPAA Privacy Rule.

[17] healthcare.partners.org/phsirb/hrchipaa.htm

[18] National Archives and Records administration Federal register, No17, volume 78, January 25, 2013

[19] About Health Insurance Portability and accountability Act, Robert M. Callif et.al.

[20] US department of Health and Human services, hhs.gov.

[21], [22]. [23], [24], [25], [26], [27] HIPAA, a practical guide to security and privacy of data, June M. Sullivan, 2008.

[28], [29], [30] US department of Health and Human services, hhs.gov, Health Insurance Privacy, summary of HIPAA security rule.

[31], [32] HIPAA, a practical guide to security and privacy of data, June M. Sullivan, published in 2008

[33] EMR and HIPAA Compliance.

[34] MPLS Fundamentals, By Luc De Ghein Nov 21, 2006