Study on HIPAA Compliance in Health IT Company and Its Application to PHI

By

Astha Billore

Dissertation submitted for the partial fulfillment of the

MBA Hospital and Health Management

Academic year, 2016-2018

The IIHMR University, Jaipur

1, Prabhu Dayal Marg, Sanganer, Airport
Jaipur 302029, Rajasthan
Ph: 0141 3924700, Fax: 3924738
Website: **www.iihmr.edu.in**

Study on HIPAA Compliance in Health IT Company and Its Application to PHI

By

Astha Billore

Dissertation submitted for the partial fulfillment of the

MBA Hospital and Health Management

Academic year, 2016-2018

IKS Health Mumbai

The IIHMR University, Jaipur

1, Prabhu Dayal Marg, Sanganer, Airport
Jaipur 302029, Rajasthan
Ph: 0141 3924700, Fax: 3924738
Website: **www.iihmr.edu.in**

INSTITUTE OF HEALTH
MANAGEMENT RESEARCH
(WHO Collaborating Centre for District Health System Based on Primary Health Care)

IIHMR UNIVERSITY

TO WHOMSOEVER MAY CONCERN

This is to certify that **Astha Billore** student of MBA Hospital and Health Management from The IIHMR University, Jaipur has undergone internship training at **IKS Health, Mumbai** from **FEBRUARY 12th 2018 to MAY 12th 2018**.

The Candidate has successfully carried out the study designated to him 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 her all success in all her future endeavors.

Dr Ashok Kaushik
Dean, Academics and Student Affairs
The IIHMR University, Jaipur

Dr Anoop Khanna
Professor
The IIHMR University, Jaipur

1, Prabhu Dayal Marg, Near Sanganer Airport, Jaipur- 302029, Rajasthan, India.
Ph.: 0141- 3924700, 2791431- 32, Fax: 0141 3924738, E-mail: iihmr@iihmr.edu.in, Web.: www.iihmr.edu.in

Date: 03rd May 2018

To whomsoever it may concern

This is in recognition that **Dr.Astha Billore,** student of IIHMR University has successfully completed her dissertation over a period of 3 months from **February 12, 2018 to May 12, 2018** at IKS Health, Mumbai.

During the period of dissertation she worked on a project "**A study on HIPAA compliance in Health IT Sector**" and was able to manage, coordinate and document the project proficiently.

She comes across as a committed, sincere and diligent individual and who has a strong zeal for learning. We wish her all the very best for her course completion.

For **Inventurus Knowledge Solutions Pvt Ltd**

INVENTURUS KNOWLEDGE SOLUTIONS PVT. LTD. 10th May 2018

Signature of respective reporting manager

For **Inventurus Knowledge Solutions Pvt Ltd**

INVENTURUS KNOWLEDGE SOLUTIONS PVT. LTD. 3rd May 2018

Signature of Human Resources

CERTIFICATE OF ORIGINAL WORK

THE IIHMR UNIVERSITY, JAIPUR

CERTIFICATE BY SCHOLAR

This is to certify that the dissertation titled "A study on HIPAA compliance and its application to PHI" with respect to IKS Health and submitted by Astha Billore Enrollment No. IIHMR U/01/2016-2018/ 0398 under the supervision of for award of MBA in Hospital Management of The IIHMR University carried out internship during the period from 12th Feb 2018 to 12th May 2018 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.

Astha Billore (15/05/18)
Signature

DECLARATION

I declare that this dissertation report submitted to The IIHMR University for MBA in hospital and health management is my personal work where any of the content presented is the result of data from a research study conducted at Health IT Company. I have not already obtained a degree in The IIHMR University or elsewhere on the basis of this work. Also, I can ensure that the work is original and to the best of my knowledge and does not breach copyright law and has not been taken from other sources except where such work has been cited and acknowledged within the text.

Signature

15/5/18

Date

ACKNOWLEDGMENT

I take this opportunity to express my profound sense of gratitude to all those who helped me throughout the duration of the project.

I would like to acknowledge, first and foremost Dr Anoop Khanna my mentor at The IIHMR University for showing confidence in me for giving me a project that helped me get well versed with the various operations in the organization and mandatory requirements for quality management. He has been a great source of knowledge, inspiration to do work with utmost diligence and sincerity

It is my radiant sentiment to place on record my best regards, deepest sense of gratitude to Dr Tapan Das and all of the support staff at Health IT Company for their careful and precious guidance which were extremely valuable for my study both theoretically and practically.

I would like to thank Mr. Hamid Batliwala my recruiter for his constant guidance throughout the project.

I would also like to thank Dr Sudip Datta (Head of HR) for allowing me to pursue internship in this esteemed hospital.

Sincerely,

Dr Astha Billore

TABLE OF CONTENTS

- Introduction
- Literature review
- Research Aim and objectives
- Research Methodology
- Results
- Conclusion
- References

INTRODUCTION

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

TIMELINE OF US LEGISTLATION

HIPAA growth since inception

- August 21, 1996

HIPAA Go by Congress Outlined principally to advanced wellbeing data trade

- 2000-HIPAA Security Control Finished by HHs

Turns into the primary government social insurance data protection law

- 2001-HIPAA Slows down

New Bramble organization revives HIPAA Security Govern remark period

- 2002-Bramble Organization Declares Support of Adjusted HIPAA

Exemptions for "treatment, instalment, and social insurance activities" included

- 2003

HIPAA Security Govern Finished

- April 14, 2003

HIPAA Security Manage Consistence Due date

- April 21, 2005

HIPAA Security Administer Consistence Due date

- 2008-Absence of HIPAA Requirement

In excess of 33,000 HIPAA protests documented with OCR to date, just 8,000 examined without any fines issued

- February 17, 2009

ARRA's HITECH Demonstration Marked into Law

HIPAA reconsidered to reinforce implementation punishments, require break notices, and extend quiet rights

- 2009-OCR Ratchets up HIPAA Authorization

A few substances fined a large number of dollars for security ruptures

- January 25, 2013

HITECH's HIPAA Change Last Control Discharged

LITERATURE REVIEW

INTRODUCTION

- HIPAA Security Run the show. Formally known as the Measures for Security of Independently Identifiable Wellbeing Data, this governs and builds up national gauges to ensure tolerant wellbeing data.

- HIPAA Security Run the show. The Security Norms for the Insurance of Electronic Ensured Wellbeing Data sets measures for persistent information security.

- HIPAA Requirement Run the show. This lead sets up rules for examinations concerning HIPAA consistence infringement.

Secured (PHI)

Secured (PHI) is any statistic data that can be utilized to distinguish a patient or customer of a HIPAA-under obligation substance. Normal cases of PHI incorporate names, addresses, telephone numbers, Standardized savings numbers, medicinal records, money related data, and full facial photographs to give some examples.

PHI transmitted, put away, or got to electronically additionally falls under HIPAA administrative gauges and is known as electronic secured wellbeing data, or e-PHI. e-PHI is managed by the HIPAA Security Control, which was an addendum to HIPAA direction established to represent changes in restorative innovation.

Components of PHI

There are 18 components of PHI

- Name
- Address
- Date
- Phone no.
- Fax
- E mail
- Social security no.
- Medical record no.
- Health design recipient no.
- Bank account no.
- Certificate or permit no.
- Vehicle identifier
- Device identifier and serial no.
- Web widespread asset locator
- Internet convention address no.
- Biometric identifier
- Full confront photographic pictures and any practically identical pictures
- Any other one of a kind recognizing no. , trademark or code.

Who should be HIPAA agreeable?

HIPAA direction distinguishes two kinds of associations that must be HIPAA agreeable.

• Covered Substances: A secured element is characterized by HIPAA direction as any association that gathers, makes, or transmits PHI electronically. Human services associations that are viewed as secured substances incorporate medicinal services suppliers, social insurance clearinghouses, and medical coverage suppliers.

Incident Management – If a secured substance or business relate has an information rupture, they should have a procedure to record the break and advise patients that their information has been traded off as per the HIPAA Breach Notification Rule. Particular insights about the HIPAA Breach Notification Rule and investigated underneath.

HIPAA VIOLATION

A HIPAA infringement is any break in an association's consistence program that bargains the trustworthiness of PHI or ePHI.

A HIPAA infringement varies from an information rupture. Not all information breaks are HIPAA infringement. An information rupture turns into a HIPAA infringement when the break is the consequence of an inadequate, deficient, or obsolete HIPAA consistence program or an immediate infringement of an association's HIPAA arrangements.

A DATA BREACH happens when one of your workers has a decoded organization PC with access to medicinal records stolen. A HIPAA VIOLATION happens when the organization whose PC has been stolen doesn't have an approach set up excepting workstations being taken offsite or requiring they be scrambled.

Legitimate Penalties for Violation

Common Penalties

— Accidental Disclosure

$100 individual/infringement

up to $25,000 every year

Criminal Penalties

— Knowing abuse of data

$50,000 and l year in prison

— False Pretenses

$100,000 and 5 years in prison

— Harmful expectation/offer data -

$250,000 and 10 years in prison

Research aim and objectives

Research aim

The purpose of this study is to understand the importance of HIPAA compliance and determine its application to 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-: In-depth interview and consultations. Total of 10 in-depth interviews were conducted, four interviews with managers of compliance team, three interviews with the training team and three interviews with virtual scribes.

DATA INTERPRETATION

A total of 10 in-depth interviews were analyzed manually for content research and following are the findings.

Protected Health Information (PHI) in Patient's chart notes

Protected Health Information implies any data, regardless of whether oral, composed, recorded, in any frame or medium that demonstrates or is identified with a person's past, present or future wellbeing status. This would incorporate any physical or emotional well-being condition, treatment or administrations gave. This data must be secured and by and large can be utilized or unveiled just with the person's authorization.

Any of the accompanying things, when utilized and joined with wellbeing data, makes PHI which is liable to HIPAA controls

1. Patient's Name and in addition name of the Insured

2. Patient/Insured's Identification codes, Address, Telephone/Fax number or email-id

3. Patient/Insured's Social Security Number (SSN)

4. Employer's points of interest and occupation

5. Finger prints, Photographs or some other distinguishing proof imprints

6. Medical history, treatment diagrams, X-Ray and other analytic reports

7. Payment subtle elements – including Bank account numbers, check/electronic settlement points of interest.

8. Dates specifically identified with understanding (aside from year), including DOB, affirmation or release date

9. Telephone Number

10. Driver's License Number

11. Email locations and FAX Numbers

12. Social Security Number

13. Medical Record/Medical Record Number

14. Health Plan Beneficiary Number

15. Account Number

16. Certificate/License Number

17. Any vehicle or gadget serial number, including tags

18. Web Addresses (URLs)

19. Internet Protocol (IP) Address

20. Finger or voice prints

21. Photographic pictures

22. Any other exceptional recognizing number, trademark, or code

23. Age more prominent than 89 (as the 90 year old and over populace is generally little)

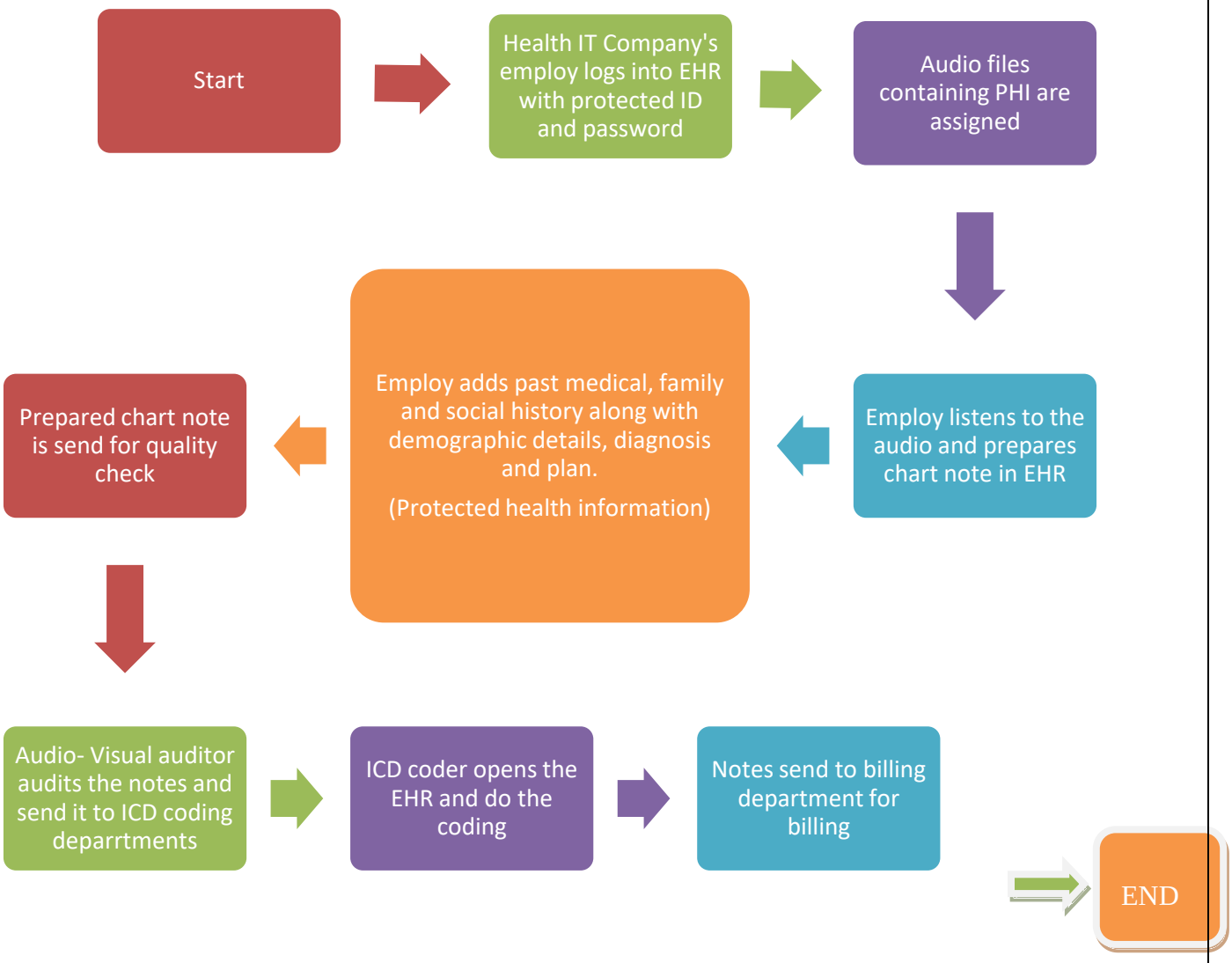
When do HIPAA rules apply to PHI?

- ✓ When chart note is in use
- ✓ When PHI is released
- ✓ When PHI is stored
- ✓ When PHI is visible on computer
- ✓ When PHI document is lying on desk
- ✓ When two providers share the PHI information
- ✓ When PHI is shared with associated service providers
- ✓ When PHI is discussed in conversation
- ✓ When PHI is discussed over a phone call.

In the event that you presume a protection infringement, inform the chief. The administration would then attempt to relieve any mischief that has happened and help anticipate future infringement.

Any staff part who strikes back against a man, who reports a potential security infringement, could be at risk for a disciplinary activity.

Process flow chart



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

- **Authorizations**

A written consent for authorization is required for all uses and disclosures of PHI.

Single 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:

1. Release of PHI for Treatment.

Example: Two providers can freely share PHI if they are both involved in the patient's care.

2. Release of PHI for Payment.

Example: A patient-accounts representative may release PHI to an insurance company to obtain payment for services.

3. PHI may be used to accomplish healthcare Operations.

Example: Procedures must be followed to maintain an audit trail to monitor access and use.

- **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

- Releasing PHI

- PHI may be released for TPO, or when appropriately authorized. The release must be done according to the standard of "minimum necessary" - only the amount of information needed to fulfill a specific purpose or accomplish a specific task.

  Example: An insurance company requests information about a patient's services that were performed in January this year. Minimum necessary would mean that you would not include information about the services that were performed in November of last year

- One must not access any information unless he or she has a justifiable, work-related reason to do so. Also, one must verify that anyone with whom you share PHI has legitimate reason to have the information

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 recognize that through my relationship with this organization I might have the capacity to see, send or potentially get secured wellbeing data (PHI), including without restriction understanding related cases data, and Medicinal Data for patients. Notwithstanding my commitments in the Business Associate in regards to such data, I consent to keep up the security and protection of such patient-related data, and concur that all such Data should be held in strictest certainty.*

I might guarantee that entrance to Persistent Therapeutic Data should be constrained to me on a "need to know" premise and that such data will be utilized exclusively for purposes identifying with interchanges with Insurance agencies, Patients, and other such gatherings associated with medicinal services tasks. I likewise consent to speedily inform my specialty head in the occasion; I wind up mindful of any infringement of this arrangement

Protecting PHI at workplace

- ✓ No patient identifying information (like patient names) should be shared within emails or Excel & Word files unless there is an explicit business reason for doing so.
- ✓ A patient account number, or an invoice number, can be used to identify accounts when required for business purposes in most cases. Please also ensure that when a patient's name needs to be included that the file must be properly encrypted before sending.
- ✓ We may sometimes receive data from clients that contain patient identifiers, please be sure to remove this information if you choose to open & save the file.

{In case if the file needs to be sent back to the client, do not share this patient information unless there is a stated business reason for doing so and, then again, make sure it is properly encrypted}

Patients' Privacy Rights

Patients have a privilege to ask for that the supplier's get in touch with them, or send them PHI, by utilizing elective methods for correspondence or an elective area.

Patients have the privilege to see copies of their own PHI archives.

Be that as it may, they don't have the privilege to get to:

- Psychotherapy notes

- Data accumulated for authoritative, common or criminal procedures

- Data that could be destructive

A patient has a privilege to ask for a rundown of all revelations of their ensured wellbeing data that are not for "TPO" that they have not by and by approved.

Patients have the privilege to ask for an alteration to their PHI.

In the event that a patient has marked an approval to discharge their PHI to an outsider, they may disavow that approval whenever.

They should deny the approval in composing by finishing a "Repudiation of Approval" Frame.

Patients have the privilege to make a composed demand for exceptional security limitations on their PHI.

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

This checklist can be used by each employ before starting the day at office.

- ✓ One User per Login Account- HIPAA requires that each staff member who accesses PHI have a unique user account and login. Logins cannot be shared. Sharing of login is a HIPAA violation. An individual is responsible for any activity that occurs under his/her login.

- ✓ 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.

- ✓ 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.

- ✓ 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.

- ✓ Collect PHI's from printers- Never leave unattended PHI on printers. Collect all PHI that you have printed as soon as possible so that no one else has access to it.

- ✓ Clean Desk Policy -

•Reduce the paper quantity that is utilized for printing ordinary.

• Carry papers just once – convert it into electronic form and discard it.

•Use secure cloud computing method to store PHI containing data.

Do not keep hard copies of mails and discard it as soon as possible.

CONCLUSION

HIPAA, formally known as Health Insurance Portability and accountability act was marked into enactment back in the 90's. These directions were ordered as a multi-layered approach that set out to enhance the medical coverage framework. HIPAA impacts pretty much everybody whether on the giving or accepting end of medicinal services.

•HIPAA helps individuals who have assemble protection scope through managers and associations.

•HIPAA helps those self guaranteed by businesses.

•HIPAA impacts social insurance laborers, from the janitorial group to doctors, for how patients are drawn closer.

•HIPAA impacts insurance agencies, medicinal services suppliers and above all, the patients.

References

- Health IT Company policies and procedures.
- HIPAA Compliance: What Has Changed and How Will It Impact Healthcare Providers? - *Bill Currier*
- HIPAA SECURITY POLICIES AND PROCEDURES- Michael Cuper
- An Investigation of Factors that Affect HIPAA Security Compliance in Academic Medical Centers- James William Brady
- An Investigation of Data Protection and Computer Security in Small Irish Medical Practices Sean McGrath
- Florida Atlantic University (FAU) - Research Integrity.
- A model for HIPAA security compliance- Author: Kathleen M Bravo
- Simkon, M. (2003, October). The CPA journal. *What businesses should know about HIPAA.* Oct.2003. Iss. Downloaded from the proQuest database on October 3, 2008.
- Simon, T. (2007). Benefits law journal. *How the final HIPAA nondiscrimination regulations affect wellness programs*. Vol. 20. Iss.. Downloaded from the proQuest database on October 3, 2008.
- MASSEY, AARON KEITH. Legal Requirements Metrics for Compliance Analysis. (Under the direction of Ana I. Antón.)
- AAMC. (2007, September). Consequences of heightened Department of Veterans Affairs information security on academic medical centers [White paper]. Retrieved May 15, 2010, from http://www.aamc.org/members/gir/whitepaperonvasecurity.pdf AAMC. (2009a). About the AAMC. Retrieved May 15, 2010, from http://www.aamc.org/about/start.htm AAMC. (2009b). GIR. Retrieved May 15, 2010, from http://www.aamc.org/members/gir/start.htm AAMC. (2009c).
- Membership. Retrieved May 15, 2010, from http://www.aamc.org/about/membership.htm AAMC. (2009d). HIPAA. Retrieved May 15, 2010, from http://www.aamc.org/advocacy/hipaa/
- Agarwal, R., & Karahanna, E. (2000). Time flies when you're having fun: Cognitive absorption and beliefs about information technology usage. MIS Quarterly,
- Aaron Massey, Paul Otto, Lauren Hayward, and Annie Antón. Evaluating Existing Security and Privacy Requirements for Legal Compliance.
- Worries over corporate reputation making information security a top priority. (2008). International Journal of Micrographics & Optical Technology,
- Wyne, M. F., & Haider, S. N. (2007). HIPAA compliant HIS in J2EE environment. International Journal of Healthcare Information Systems and Informatics

- Wicke, S. (2003). Training the troops for HIPAA compliance: Are you ready? Journal of Health Compliance,