Breaches and the impact on the organization

HIPAA INSTITUTE

Achieve | Maintain | Inculcate | Track

INTRODUCTION

Every patient trusts that their therapeutic and other medical records are confidential and will be protected. They should be aware who can access this data, when it is stored with the healthcare provider. The **Privacy Rule (Federal law)** gives you rights over your medical records and sets principles and breaking points on who can take a view at and get your medical record. The Privacy Rule applies to all who have ensured medical records, whether electronic, composed, or oral. The **Security Rule** is a Federal law which ensures security for medical records in electronic form. These rules are to be followed by **health plans, healthcare clearinghouses**, and **any healthcare provider and their business associates** who transmit health information in electronic form.

The Health Insurance Portability and Accountability Act of 1996 **(HIPAA)** in United States is a legislation that provides data privacy and security provisions for safeguarding medical information. If an organization does not implement these rules, it is under a **Breach**. The breach notification obligations differ based on whether the breach affects 500 or more individuals or fewer than 500 individuals. If the organization is under HIPAA and not following these rules it's under "Danger."

The rules that the organization should follow to avoid HIPAA violations are as follows:

The HIPAA Privacy Rule The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and healthcare transactions electronically.

The HIPAA Security Rule The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity

The Enforcement Rule The HIPAA Enforcement Rule contains provisions relating to compliance and investigations, the imposition of civil money penalties for violations of the HIPAA Administrative Simplification Rules, and procedures for hearings.

The Transactions and Code Sets Rule The HIPAA Transactions and Code Set rules is meant to bring standardization in the electronic exchange of patient-identifiable health-related information

The Unique Identifiers Rule (National Provider Identifier (NPI) NPI is a unique identification number for all covered entities. HIPAA-covered entities must use only the NPI to identify covered healthcare providers in standard transactions.

BREACH SURVEY

According to the survey, the following breaches have been reported from 2009 to 2016 in different parts of United States.

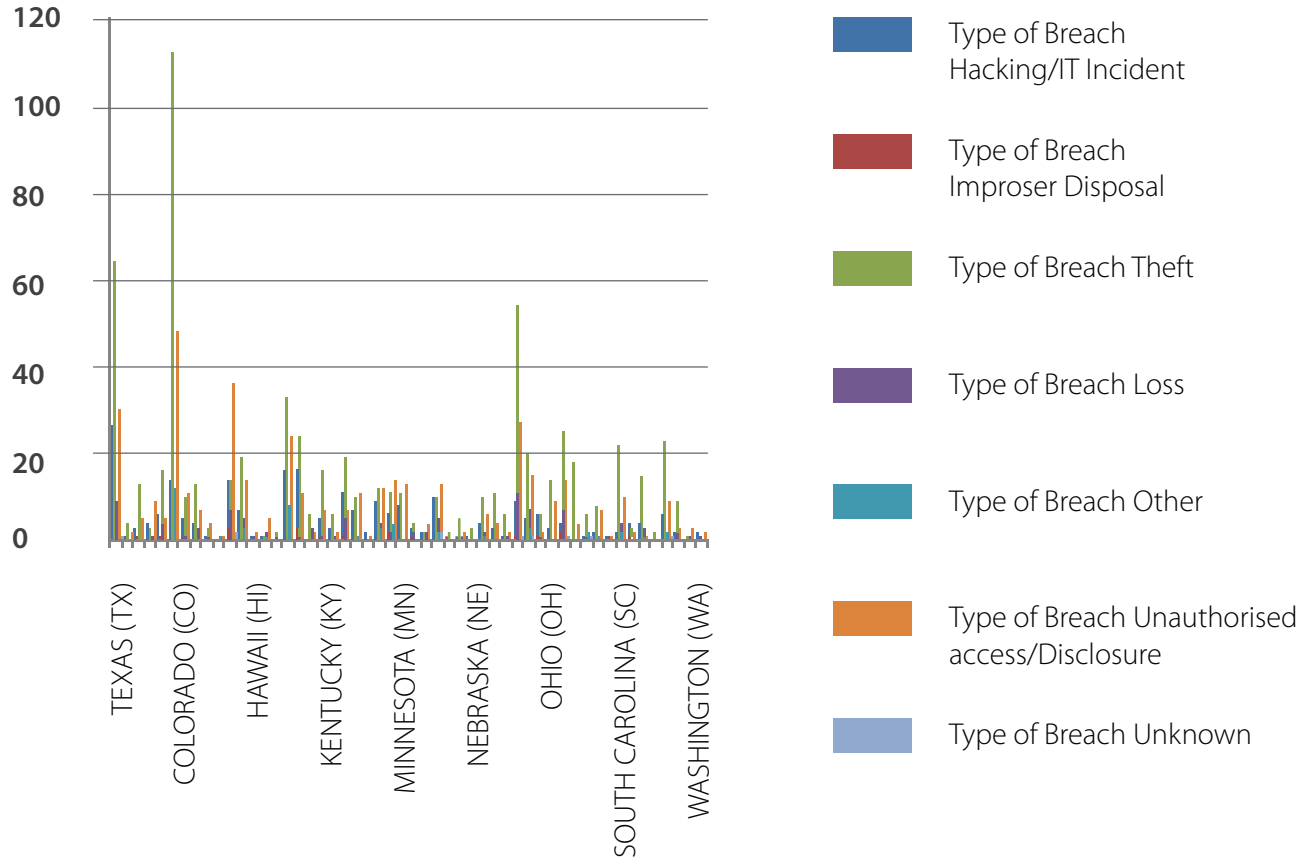

Figure 1: Breach survey in USA (2009-2016). x axis:States in USA y axis: Number of breaches that has been reported in healthcare sector. Source: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Figure 1 denotes that the most common breach in the health plans, healthcare clearinghouses, healthcare provider and business associates are Theft , Unauthorised access/disclosure and Hacking/IT incident.

TABLE 1: Types of breach and the impact on the organization

S No.	Breach	Forms of breach	Impact
1.	Employees disclosing information	Gossiping and sharing any patient information by the employee	Significant penalty
2.	Medical records mishandling	Accidentally leaving written patient charts in the patient's examination room available for another patient to see	Warning to the staff and penalty
3.	Lost or stolen devices	Theft of PHI (protected health information)	Fine
4.	Texting patient information	Texting confidential information to unauthorized number or person by the employee	Significant penalty
5.	Social media	Posting patient photo on social media with patient name and doctor's specialty	Significant penalty
6.	Employees illegally accessing patient files	Accessing patient information by unauthorized person	Fines and even prison
7.	Social breaches	Inquiring at a social setting about their friend who is a patient in a clinic with the healthcare provider	Illegal and/penalty
8.	Authorization requirements	Written consent , disclosure of any individual's personal health information without prior authorization	Significant penalty
9.	Accessing patient information on home computers	Most clinicians use home computers after clinic hours, and it is breach if the screen is accidentally left on and a family member retrieves the data from the computer.	Significant penalty
10.	Lack of training	An employee who is not familiar with HIPAA regulations who has access to patient information	Penalty and cancelation of license

According to the data, the following are the top 10 companies with the number of healthcare record breached from 2010 to 2015 in different parts of United States.

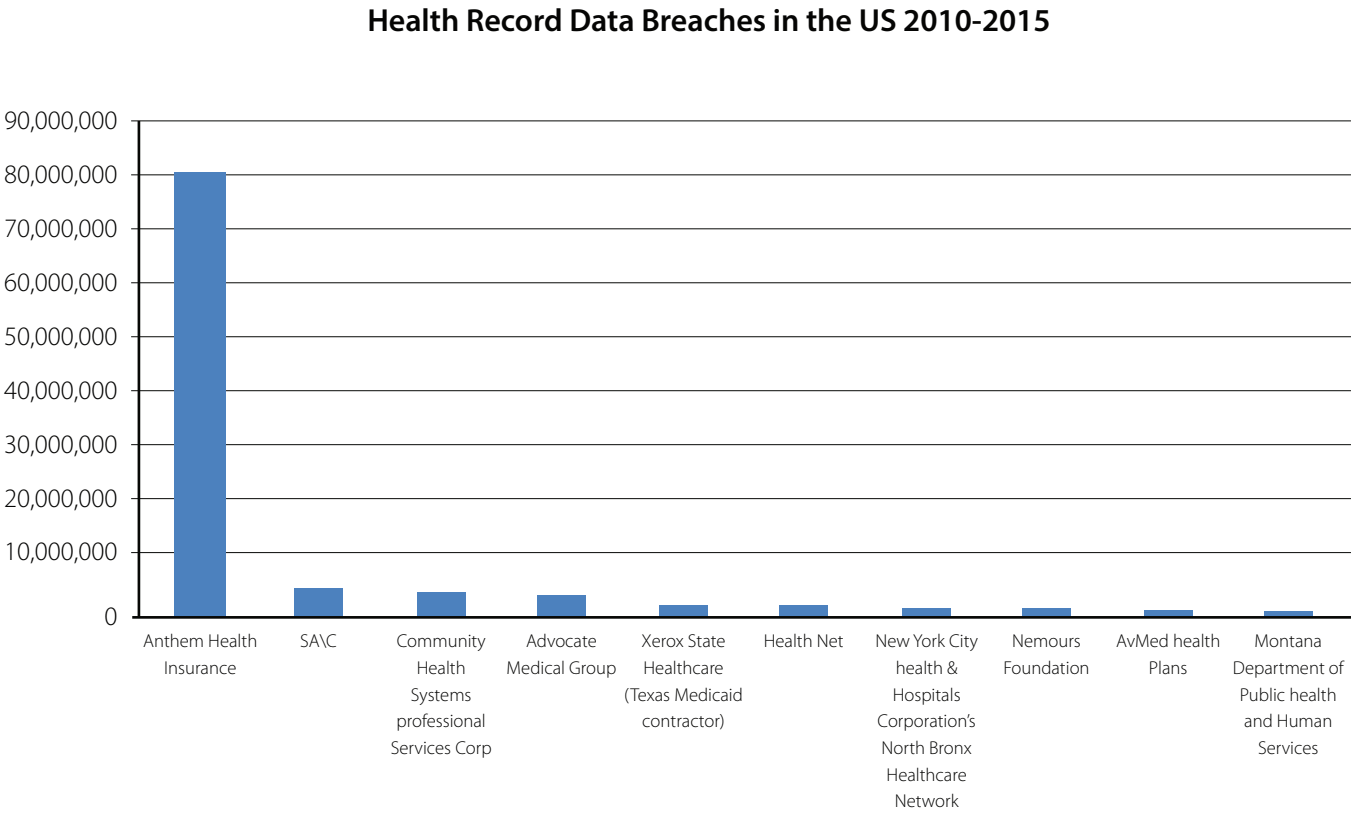

Figure 2: Health record data breaches in the US 2010-2015 x axis: Names of the companies y axis : Number of health records breached. Source: http://www.vaxchoicevt.com/wp-content/uploads/2015/03/Health-Record-Data-Breaches-in-the-US-2010-2015.xlsx

The Impact on the Organization on Violating Rules

Many data breach lawsuits are filed against healthcare organizations, and either they are actually found guilty or they choose to settle. However, when settlements over large breaches do occur, they can be hugely expensive for companies and health systems. Fines serve as reminders of just how vulnerable patients' protected health information is in the age of cyber attacks. Audits are routine in the healthcare industry; if the documents that an organization presents to the auditor do not meet the requirements of audit then the organization is penalized or in some cases the license gets canceled.

Case-1

Healing Center Implements New Minimum Necessary Polices for Telephone Messages

Category: General Hospital

Issue: Confidential Communications

Case: A doctor's facility worker did not watch least essential prerequisites when she cleared out a phone message with the daughter of a patient that mentioned restorative condition and treatment plan. An investigation also indicated that the confidential communications requirements were not followed, as the doctor's facility worker left the message at the patient's home telephone number, regardless of the patient's directions to get in touch with her through her work number.

Case-2

Health Maintenance Organization Revises Process to Obtain Valid Authorizations

Category: Health Plans

Issue: Impermissible Uses and Disclosures; Authorizations

Case: A complaint alleged that a health maintenance organization impermissibly disclosed a member's data, when it sent her entire medical record to a disability insurance company without her authorization.

Case-3

Mental Health Center Corrects Process for Providing Notice of Privacy Practices

Category: Outpatient Facility

Issue: Notice

Case: A psychological wellness center did not provide a notice of privacy practices (notice) to a father or his minor daughter, a patient at the center. In response to an investigation, the psychological wellness center acknowledged that it had not provided the complainant and his daughter with a notice prior to her mental health evaluation.

An organization can be disassembled or may be slapped with fine as a consequence of non-compliance with regulations regardless of whether the violation was unintentional or result of wilful negligence.The civil and criminal penalties are huge. Healthcare providers can also be at risk for loss of license. The organization also has to incur the cost of implementing a corrective action plan to address the rules. All medical staff that access patient health information must be trained and retrained on proper HIPAA procedures. Documentation of provided training is required to be kept for six years. **Protecting your practice means protecting your reputation.** The number of health care organizations with major breaches and receiving substantial penalties is growing at an alarming rate and it has reached a point where there is a large risk of losing so many clients that these organizations may not be able to bounce back. **To keep every cog and wheel is the first precaution of intelligent tinkering.** This can be achieved by HIPAA Institute Services and Products which are powerful and user friendly. It can be implemented to avoid Breach. The motto of HIPAA Institute is to help health plans, healthcare clearinghouses, and any healthcare provider and their business associates by making it easier

to establish and maintain an effective compliance program.

One of the solutions can be:

HIPAA Institutes offers various levels of compliance solutions to adhere the regulatory requirement and also, meet the needs of the organization like Automated Compliance tool, End-to-End Risk Governance, which includes Risk Assessment, Risk analysis and Risk Management.

It also facilitates templates, checklist, auditing tools and access to training resources, example, **"Vulnerability Assessment checklist", "Compliance Wizard and Risk Assessment Master", "On-Site HIPAA Inspection Checklist",** and many more products and services.

HIPAA
INSTITUTE

Achieve | Maintain | Inculcate | Track

For More Information

Call us at : **1-800-262-8146**
Visit us at : **www.hipaainstitute.com**
E-mail us at : **help@hipaainstitute.com**