




# **SERVICE METHODOLOGY FOR HIPAA**

**Health Insurance Portability  
and Accountability Act**

## INTRODUCTION TO HIPAA


HIPAA is a comprehensive federal law enacted to:

- 
- Protect the privacy of a patient's personal and health information
  - Provide for electronic and physical security of personal and health information
  - Standardize coding to simplify billing and other transactions
- The Health Insurance Portability and Accountability Act (HIPAA) involve Privacy, Security, and Breach Notification Rules protect the privacy and security of health information and provide individuals with certain rights to their health information.
- The Privacy Rule which sets national standards for when protected health information (PHI) may be used and disclosed
  - The Security Rule, which specifies safeguards that covered entities and their business associates must implement to protect the confidentiality, integrity, and availability of electronic protected health information (phi)
  - The Breach Notification Rule, which requires covered entities to notify affected individuals; U.S. Department of Health & Human Services (HHS); and in some cases, the media of a breach of unsecured PHI.

## KICKOFF

Kickoff meeting is an essential tool to communicate and plan for the execution of the project with minimal obstruction and to complete the project within planned time and cost.

Agenda for the kick off meeting is:

- 
- Project plan discussion: This includes discussion about accountability and responsibility of stakeholders, milestones and deliverables in the project.
  - Scope of services
  - Legal and regulatory requirements

## CREATION OF CORE TEAM

- Appointment of CISO
- Appointment of Information Security Management Committee.
- Appointment of HIPAA Security officer

## HIPAA AWARENESS TRAINING

HIPAA awareness training will be conducted to the employees of your organization. The training session is to help employees to gain knowledge, understand the concepts of HIPAA, and align processes and practice towards achieving and establishing, implementing, maintaining and continually improving a service management system work environment. When staffs have been trained they can think & act and contribute towards achieving the goals.

## PHASE WISE IMPLEMENTATION

### PHASE I - GAP ANALYSIS

During this phase we conduct a gap analysis to check how much of your current practices are in line with the requirements. Your current practices are verified against these four reference criteria.

- HIPAA standard requirements
- Legal, Regulatory and Statutory requirements

The results of this analysis are presented in the form of a Gap Analysis Report. This report acts as the list of action items for the remainder of the project.

## **PHASE II - PERFORMING HIPAA RISK ASSESSMENT**

A Risk Management procedure shall be documented and used as reference to manage the identified risks in consultation with all process owners function heads. We use risk management techniques like ISO 31000, ISO 27005, NIST, COBIT to identify, analyze, evaluate, document, prioritize, treat quantify the identified risks. This step creates a Risk Register. Suitable Risk treatment plans are identified and implemented based on the risk appetite of the company, The outcomes of such actions are calculated, recorded, evaluated and documented. Periodic risk audits are being carried in order ensure the adherence of the system to the compliance.

## **PHASE III - DEVELOPING HIPAA REMEDIATION PLAN**

Post risk assessments we assist in designing of HIPAA remediation plan based on the risk assessment results this is mainly done by coordinating with functional heads in order to implement in efficient manner an effective, HIPAA-compliant Remediation Plan typically will include,

- What needs to be done to properly secure your private patient data
- A realistic time-frame for these tasks to be completed
- A list of which members of your team are responsible for which tasks
- Documentation of follow through or completion of these tasks

## **PHASE IV - DEVELOPING BUSINESS ASSOCIATE CONTRACT AGREEMENT**

Under HIPAA, persons or entities outside your workforce who use or have access to your patient's PHI or phi in performing service on your behalf are said to be "Business Associates" we assist in developing and reviewing of Business associates contract agreements based on the type of vendor who is being engaged for a specific services with respect to HIPAA Compliances.

## **PHASE V - SETTING UP PROCESS FOR DATA BREACH INCIDENTS**


We assist in Setting up the processes to identify and handle PHI Data breaches. (Eg. HIPAA breach notification procedures) and also assist in developing procedures on incident reporting mechanism to the concerned supervisory authority.

## **PHASE VI - HIPAA DOCUMENTATION SUPPORT**

The HIPAA Compliance Plan should include Policies and Procedures ensuring the Privacy of Protected Health Information and the Security of such information. The Security Policies and Procedures deal with phi (electronic PHI) we assist in developing of HIPAA privacy and security policies and procedures for each function by understanding the type of (phi) they handle with respect to HIPAA.




## HIPAA SECURITY OFFICER INTERNAL AUDIT TRAINING




HIPAA Internal Auditor (IA) Training will be provided to the HIPAA Security officer. This training will equip such personnel to analyze the need for IA, plan and schedule IA, prepare audit checklists, and conduct an IA and to document and report their observations to the top management

## HIPAA INTERNAL AUDIT



Our experts will oversee the conducting of internal audit by your HIPAA security officer. This internal audit will identify still existing gaps in the system and demonstrate the level of preparedness to face the compliance audit. This audit gives the organization a chance to identify and rectify all non-conformances before proceeding to the compliance audit. The top management is notified of the internal audit findings.

## HIPAA - ROOT CAUSE ANALYSIS (RCA) AND CORRECTIVE ACTIONS



All non-conformances identified during the internal audit, client or third party audits, or from Risk Register, Vendor risk assessments, Incident logs, Data Backup logs, Data Breach notification reports, Vulnerability Assessment & Penetration Test (VAPT), Data retention logs and any other sources have to be listed. RCA is performed using techniques like Brainstorming and Fish-Bone methods. The optimal correction and corrective actions are implemented and the effectiveness of such actions is documented and reviewed via a HIPAA Corrective Action Report (CAR).

Our experts will be present with your team to guide through the process.

## HIPAA MANAGEMENT REVIEW MEETING (MRM)

The MRM is an opportunity for all stakeholders to meet on scheduled intervals to review, discuss and plan actions on the below agenda points.

- Risk register
- Deviations on compliance aspects
- Post-delivery activities reports
- Action plan to resolve any open items
- Opportunities for improvement, changes needed in the system

## HIPAA COMPLIANCE AUDIT

When the levels of preparedness have reached adequate levels, the process for Compliance certification begins. An appointed auditor of the Compliance Body (CB) verifies the preparedness via an External audit. This involves the auditor reviewing the policies, processes, SOP's, critical operational records, and IA and MRM records. Any major deviations from the CB's expectations will be notified at this point for bringing in the necessary corrections. This reduces the chances of major non-conformances during the certification audit. TOP Certifier will by liaise with all stakeholders and oversee smooth completion of the audit.

## CONTINUATION OF COMPLIANCE

TOP Certifier will be part of your organization's compliance journey and assist you at regular intervals with necessary trainings, system support and pupations, internal and external audits and regular renewal of your certification.