Awareness
to
ISO 27001:2022
&
HIPAA
Health Insurance Portability and Accountability Act

HIPAA ?

Health Insurance Portability and Accountability Act Is a civil rights law passed in 1996 is a federal law designed to protect a subset of Sensitive Information known as protected health information (PHI).

HIPAA was expanded and strengthened by the HITECH Act (Health Information Technology for Economic and Clinical Health).

PHI ?

Any information that can be used to identify a patient – whether living or deceased – that relates to the patient's past, present, or future physical or mental health or condition, including healthcare services provided and payment for those services.

The Privacy Rule

Provides federal protections for protected health information held by covered entities (CHS) and gives patients an array of rights with respect to that information. At the same time, the privacy rule is **balanced** so that it permits the disclosure of protected health information needed for patient care (treatment) and other purposes such as payment and healthcare operations.

Forms of PHI

Written information
Oral communication
EPHI

The Security Rule

Specifies a series of administrative, physical, and technical safeguards for covered entities to use to assure the confidentiality, integrity, and availability of **electronic** protected health information

HIPAA Security Rule

Confidentiality means that data or information is not made available or disclosed to unauthorized persons or processes.

Integrity means that data or information has not been altered or destroyed in an unauthorized manner.

Availability means that data or information is accessible and useable upon demand only by an authorized person.

What HIPAA Does ?

1. Creates standards for protecting the privacy of health information
2. Protects and enhances rights of patients by providing them access and control of their information
3. Creates standards for the security of health information
4. Creates standards for electronic exchange of health information
5. Requires action as single entity
6. Mandates training for workforce members on standards and policies

Technical Safeguards

1. Access Control
2. Audit Controls
3. Integrity
4. Person / Entity Authentication
5. Transmission Security

Physical Safeguards

1. Facility Access Controls
2. Workstation Use
3. Workstation Security
4. Device and Media Controls

Administrative Safeguards

1. Security Management Process
2. Assigned Security Responsibility
3. Workforce Security
4. Information Access Management
5. Security Awareness Training
6. Security Incident Procedures
7. Contingency Plan
8. Evaluation
9. Business Associate Contracts and Other Arrangements

Employees Must Report Breaches (Incident Reporting)

Part of your responsibility as an employee is to report privacy or security breaches involving PHI to any one of the following persons:

The Chief Compliance Officer – Mr. Saajan Thomas
The HIPAA Privacy Officer – Mr. Sudhir Dudhane
The HIPAA Security Officer – Sysadmins

Some key steps that everyone Should include

- Use good, cryptic passwords that can't be easily guessed
- keep your passwords secret
- Make sure your computer is protected with up-to-date anti-virus and anti-spyware software
- Don't click on unknown or unsolicited links or attachments, and don't download unknown files or programs onto your computer.
- To help reduce the risk, look for "https" in the URL before you enter any sensitive information or a password (the "s" stands for "secure").
- Remember that information and passwords shared via standard, unencrypted wireless or verbally are especially easy for anyone to intercept or to misuse.
- Security depends on people more than on technology
- Make Sure that you have locked the desktop Screen before leaving the work area

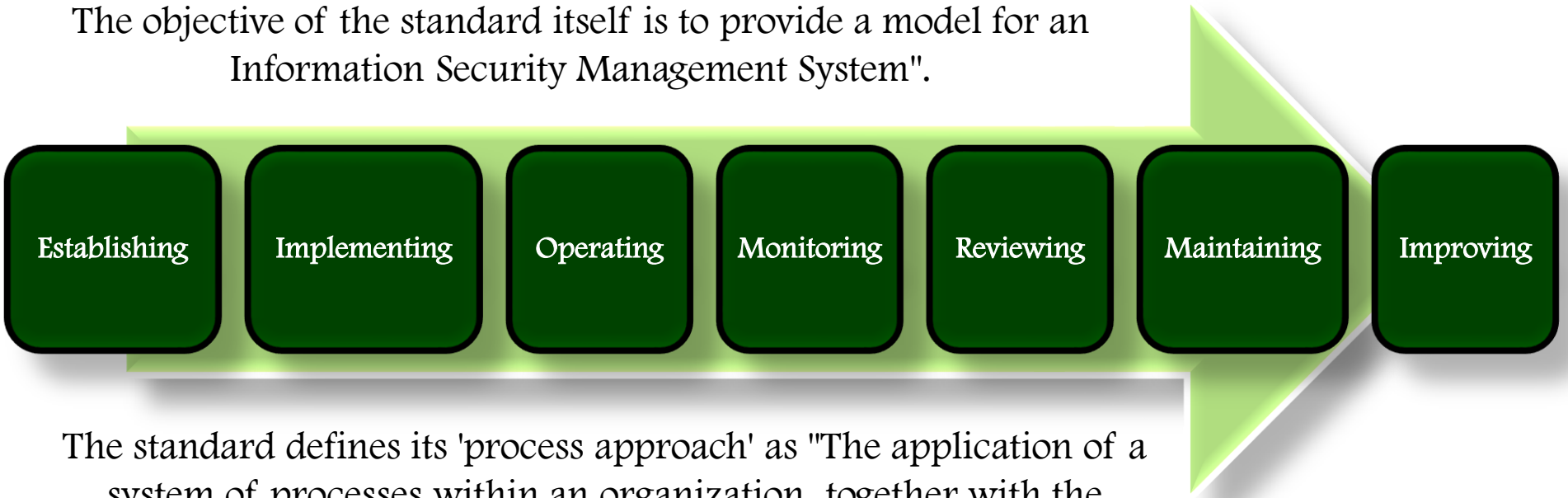
At Neural IT Pvt. Ltd.

- Users will prevent unauthorized access to their e-mail accounts by using passwords.
- Users will be responsible for any activity on their account.
- It is strictly prohibited to use or force entry into another user's e-mail account without permission.
- Employees who receive virus warnings must NOT distribute these warnings. Instead, Information Systems must be contacted immediately and Support Desk staff will investigate and take action.
- Files over 3 MB should not be sent as e-mail attachments.
- Mass distribution of forwarded e-mails from any source such as, jokes, trivia, stories, animated greeting cards and promotional material will not be sent through the e-mail system.
- Users will not forward chain letters to other staff members.

ISO 27001 ?

The ISO 27001 standard is the specification for an ISMS

The objective of the standard itself is to provide a model for an Information Security Management System".



The standard defines its 'process approach' as "The application of a system of processes within an organization, together with the identification and interactions of these processes, and their management".

Why ISO ?

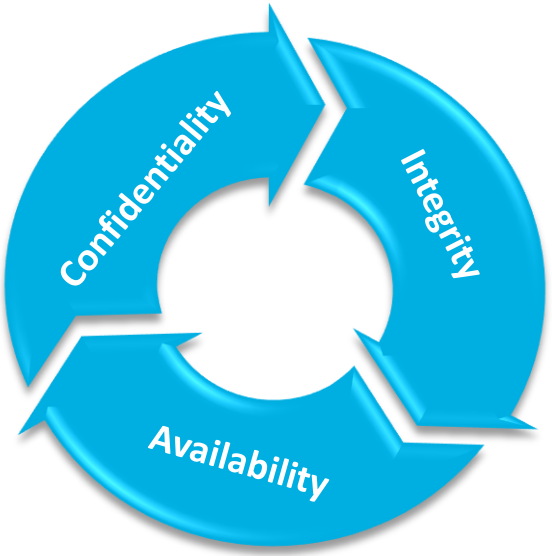
- Reduces Time
- Uses Best Methods
- Drives forward improvement process
- Prevents problems from reoccurring
- Improves employee performance
- Provides Standard Frameworks.

Confidentiality
Integrity
Availability

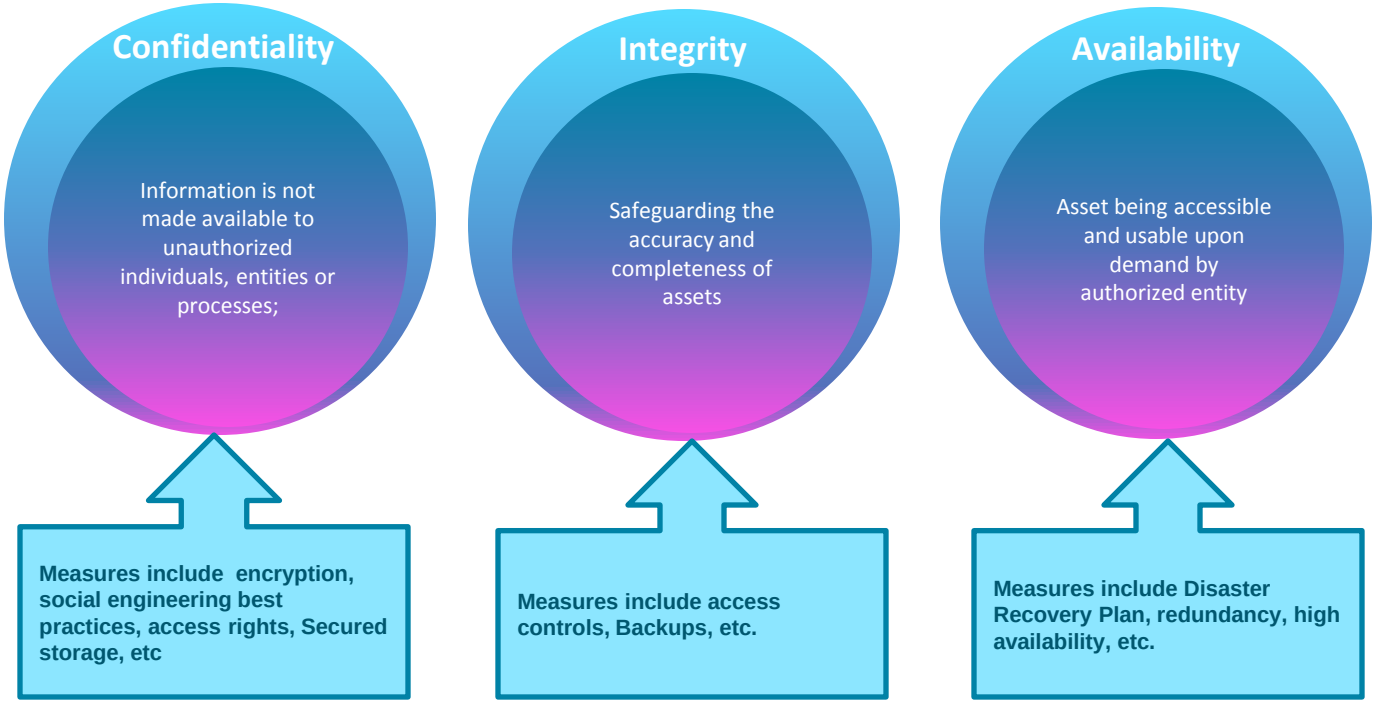
What is Information Security ?

Neural IT
Simplifying Thought

*"Information security is protecting the information through preserving their **Confidentiality**, **Integrity** and **Availability** along with the authenticity and reliability"*



Information Security Triad ?



Information Security – Who is responsible ?

Password Security

Neural IT
Simplifying Thought

Do's

- Keep your passwords secret
- As per policy, password should be min 8 characters with alphabets, numbers, and special characters (#, @, *, $, &, %,)
- Use passwords that are easy to remember but difficult to guess
- Change passwords every 90 days to avoid password expiry

Don'ts

- Don't use passwords which are based on your personal info or words found in dictionary
- Don't write down or store passwords
- Don't share your passwords with anyone
- Don't reveal passwords in email, chat or other communication

How long it takes to crack a Password ?

Neural IT
Simplifying Thought

Length	Lowercase	+Uppercase	+No. & Symbols
6 Characters	10 Mins	10 hrs	18 days
7 Characters	4 hrs	23 days	4 years
8 Characters	4 days	3 years	463 years
9 Characters	4 months	178 years	44,530 years

Malware Protection

Malware is a 'Malicious Software' which is developed with intentions to cause harm to Confidentiality, Integrity and Availability of Information

Some common Malware are Virus, Worms, Trojans, spyware

Ensure that the Antivirus is running on your desktops

In case the antivirus is not present or not functional, report it immediately to IT service desk

---

Scan all files coming from external sources (such as email, internet, USB).

Do not open or download any executable files (.exe) from email attachment

Spam

Spam is an unsolicited e-mail broadcasted indiscriminately to multiple mailing lists, individuals or news groups

- Never reply to a spam or share any personal information
- Don’t buy anything from a spam mail
- Be careful while opening an email attachment if you suspect it to be unusual
- Share your e-mail address only with people you know
- Don't forward an email from someone you don't know to a list of people.

Email Security

Do’s

- Use Email only for business purposes
- Use only official email ids for official purposes
- Retain important emails for evidence/record purposes

Don'ts

- Transmitting offensive material like political opinion, pornography and sexual harassment material;
- “Spamming” unsolicited messages, promotions, sending or forwarding chain letters;
- Creating, sending, receiving or storing materials that infringe the copyright or other intellectual property right of any third parties;

Clear Desk & Clear Screen

Neural IT
Simplifying Thought

Do's

- Lock your desktop while leaving work place
- Ensure your desk is clear and no sensitive information lies around
- Be aware of shoulder surfers in office or in public places
- Be cautious while handling sensitive information
- Shred unwanted documents

Don'ts

- Don't forget to collect your printouts from printer
- Don't forget to clear white board while leaving meeting rooms
- Don't use / install any unauthorized software

Social Engineering

Neural IT
Simplifying Thought

Avoid discussing sensitive information with others in public

Do not give out sensitive information over email/telephone without proper verification of identity.

Always be assure of the other person's identity, when you receive a call which you are not expecting

When discussing any important business issue make sure no one else is listening

Physical Security

Neural IT
Simplifying Thought

Control Implemented

- Security guards and various access control system put in place

Guidelines to be followed

- Server room door ..... Keep it closed
- Access control card ..... Use it , do not share it
- Always wear your identification and access badge
- Escort a visitor / vendor to work / sensitive area
- Never leave the entry gate open
- Tail-gating / Piggy-backing should be discouraged
- Never share your ID card with others

Display your ID badge prominently

Information Security Incidents

A Security Incident means a real or potential security event which causes harmful impact to business operations or users.

- Virus and spyware hacking attempts
- System malfunction
- Loss or theft of data
- Either failed or successful attempts to gain unauthorized access to data
- Violation of Neural IT’s security policy

Information Security Incidents Reporting

Neural IT
Simplifying Thought

Do’s

- Report security incidents
- Contact: Sysadmin department for all IT related security incidents
- Contact the HR/Admin team for all Physical Security related security incidents

Don'ts

- Don’t discuss security incidents with anyone outside Neural IT.
- Don’t attempt to prevent anyone from reporting the incident
- Never talk to media person unless authorized


Think Safe.
Act Safe.
Be Safe.
SAFETY