It's all about protecting our data!

INFORMATION LAWS & STANDARDS

As an organizaton, it is the responsibility of every employ to secure and protect the information that we use, share, and create.This infograpic has been created to help to provide a simple understand of the laws and standards required to do so.

WHAT IS CLASSIFIED AS DATA?

Data can be any information that has been created, can be stored, or transmitted. This includes numerical values, characters, or a combination of the two.

WHAT INFORMATION IS IMPORTANT?

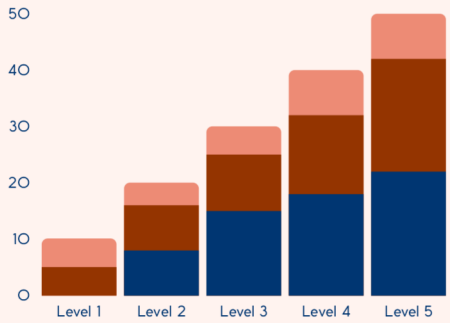
Contrary to what some may believe any information no matter how significant should be considered important and should be handled with care. Proper security of usable data and the disposal of unusable data should always following the laws and standards that govern the handling of information.

Handling of sensitive data

All sensitive information should be encrypted and stored in a securely locked place

Understanding information by levels of importance

- **Level 1** - information considered as viewable by the public
- **Level 2** - information which is considered classified
- **Level 3** - information that could cause risk or material harm to an individual or an institution such as students or universities
- **Level 4** - information that consist of PII (Personal Identifiable Information), credit card data, and medical information
- **Level 5** - information that if compromised could cause irreparable damage or harm to an individual. This may include psychological, reputational, & financial.



Supporting details

For any questions and assistance with understanding these levels, please contact the human resources and/or the information security department.

Related Information

All users are to secure that laptops with cable locks if leaving them at their desk, and should always lock their computers before leaving their desk.

NOTABLE LAWS

GRAMM-LEACH-BLILEY ACT

(GLBA)

Requires financial institutions - companies that offer consumers financial product or services like loans, financial or investment advice, or insurance - to explain their information-sharing practices to their consumers and to safeguard sensitive data.







SAFEGUARD RULE

Within the Gramm-Leach-Bliley Act financial institutions must protect the consumer information they collect.

Protecting customers information is not limited to information collected in person but is also extened to online banking information collected as well.

Related Information

Consumer information is to only be shared with the consent of the consumer. Any information that may be used by the company that will be shared with a third party must be approved by the owner of the information.

NOTABLE LAWS

SARBANES-OXLEY ACT

TITLE I: PUBLIC COMPANY ACCOUNTING OVERSIGHT

- Oversees the audit of public companies that are subject to the securities laws
- Establish audit report standards and rules
- Inspect, investigate, and enforce compliance on the part of registered public accounting firms, their associated persons, and certified public accounts.

Public Companies

There are many companies that are governed by these laws. This include companies like Charles Swab, Coinbase, Savings & Loans, etc.

Oversight

The companies are subject federal oversight to insure best practices and compliance with securities laws and standards.Thes companies are subject to several audits a year and may be required to provide additional information such as tax records and profit and lost statements.

Related Information

All users are to secure that laptops with cable locks if leaving them at their desk, and should always lock their computers before leaving their desk.

Who's fall under this guidance?

The laws and standards does not just apply to the company or institution in their place of origin, but is extended to other aspects of the business and it associates locally and abroad.

Compliance

Every company which are subject to this law is expected to comply with every aspect of the law in order to continue actively due business.

NOTABLE LAWS

HIPAA PRIVACY & SECURITY RULES

Is list of rules that governs the sharing of and person's health or medical information either verbally or electronically,





What protected?

HIPPA establishes national standards for protecting of certain health information

Confidentiality

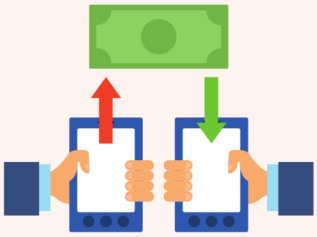
The complexity of HIPAA rules required a patient to have to grant permission to the healthcare provider to share information with other physician and/or a family member including spouses.

Security around electronic sharing of information and storage

HIPAA laws and rules also require healthcare providers to protect patients information in the process of storing and/or electronically submitting or sharing. Whether it be via email, or cloud storage.

What else is protected?

Under the HIPAA Privacy & Security Rules, other information such as health plans, health care clearing houses, or any form of transactional information done by or with a healthcare provider.



PCI DSS

THE PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

As list of standards that was created by the MasterCard, Visa, Discover Financial Services, JCB International, and American Express. And is governed by the Payment Card Industry Security Standard Council.

What is protected?

The PCI DSS is put in place to govern all transaction around both credit and debit cards.

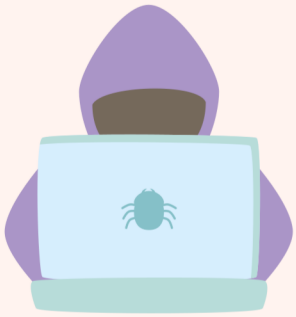
PCI DSS Mission

PCI DSS mission is to not only protect and govern transactions around debit and cards. It mission is to support services which drive education, awareness, and effective implementation by stakeholders. This can be any company, and or individual that provide a service or business that will allow for transactions using either form of payment mention above.

THE COMPUTER FRAUD & ABUSE ACT

(CFAA)

The federal computer fraud law prohibits intentionally accessing a computer without authorization . This act comes with very harsh penalties and malleable provisions.



ELECTRONIC COMMUNICATION PRIVACY ACT

(ECPA)

Is a law the has been put in place to the privacy expectations of citizens and the legitimate needs of law enforcement. The include the protect from electronic eavesdropping and wiretapping.

Wiretap Act & Stored Communications Act & Pen Register Act

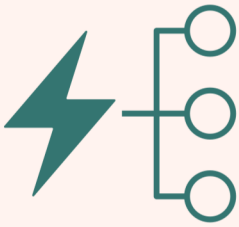
Expresses that wiretapping and electronic interceptions aided by wire, cable, or other like connections are prohibited. The law is not extended to oral communications exhibiting an expectation that such communications is not subject to interception under circumstances justifying such expectation.

What are the consequences

Any violator of this law is subject to a $250,000 fine and/or up to five years in prison and any recover damages. This could also lead to the offender pay additional fees in punitive damages and attorney fees.

NERC CIP

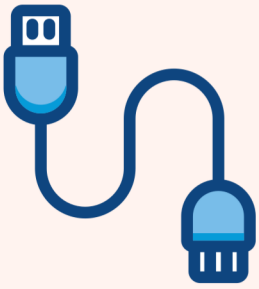
The NERC CIP laws and standards provide mandatory security standards that apply to entities that own or manage facilities that are part of the U.S. and Canadian electric power grid.



NERC Standards

The NERC CIP included several different standards such as:

- **Asset Identification & Classification**
  - Facility Classification
  - Asset Identification
  - Inventory Approval
- **Policy & Governance**
  - Designation of Senior Responsible Official
  - Policy Creation & Maintenance
  - Policy Creation & Maintenance for Low-Impact Assets
- **Personal & Training**
  - Security Awareness
  - Background Checks
  - Training
  - Access Management
  - Access Review
- **Network Security**
  - Creation of Electronic Security Perimeters or Virtualized Equivalents
  - Management of Secure Interactive Remote Access
- **Physical Security of Cyber Assets**
  - Physical Security Plans
  - Creation & Monitoring of Physical Security Perimeters
- **System Security Controls**
  - Patch Management
  - Management of Ports and Services
  - Malware Prevention
  - Security Event Logging
  - Management of Shared Accounts
  - Password and Credential Management
- **Cyber Security Incident Response**
- **Recovery Plans**
  - Continuity of Operations
  - Backup & Restoration



US PATRIOT ACT

US PATRIOT ACT (SECTIONS 808, 814, 816)

Following the events of surrounding the September 11, 2001 attack on the world trade centers, the US Patriot Act was establish to protect the US from future terrorists attacks, through the interception of information surrounding surveillance either physical, digital, or electronically.

Sec. 808

Deals with the definition of federal crime and terrorism. This section provides the guidelines surround determining who can be classified as a terrorist either domestic or abroad.

Sec. 814

Deals with the deterence and prevention of cyber terrorism. This section provides the guidelines surround determining what can be considered as cyber terrorism and the legal ramifications surrounding cyber terror and the government's rights to prosecute offenders.

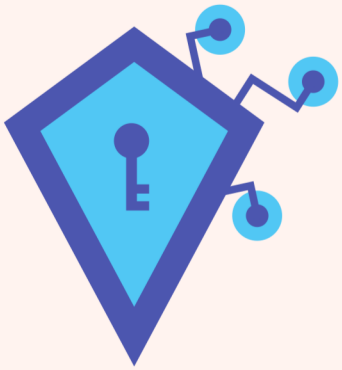
Sec. 816

Deals with the development and support of cybersecurity forensic capabilities. This section provide the guidelines in the government's and law enforcement's ability to gather and obtain any information and property that may have been apart of or suspected of being apart of a cyber security threat or offense.

STANDARDS

NIST

Is is a government entity that is responsible for setting the standards and guidelines surrounding cybersecurity. This includes both government entities and the private sector. NIST provides 18 different standards for governing the protection of computer networks, mobile devices, and network infrastructures.



NIST Standards

The NIST Standards include plans to focus more on and include cryptography, education and workforce, emerging technologies, risk management, identity and access management, measurements, privacy, trustworthy netoworks and trustworthy platforms.