Hello Everyone, in this video, you will learn about various Information Security standards followed in India and other countries to regularize the protection of information and other assets.

Let's understand the cyber security standards first. To make cybersecurity procedures clear and more efficient in any organization, the written rules, prescribed by any standardization body are required. These rules are known as cybersecurity standards.
These standards may involve methods, guidelines, reference frameworks, etc. to ensures efficiency of security and provide the structure for new developments.

The most commonly used Information security standards are Payment Card Industry Data Security Standard (PCI-DSS), ISO/IEC 27001:2013, Health Insurance Portability and Accountability Act (HIPAA) 1996 and COBIT. Let's discuss about them one by one.

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards.
PCI DSS applies to all entities involved in payment card processing - including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data.

The PCI DSS standard specifies twelve requirements for compliance, which are organized into six groups called control objectives. These control objectives are

- Build and Maintain a Secure Network
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy

ISO/IEC 27001:2013 is an information security standard published by ISO and IEC subcommittee jointly. It specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It enables organizations of any kind to manage the security of assets such as financial information, intellectual property, employee details or information entrusted by third parties. It has been defined using 114 controls in 14 groups with 35 control objectives.
More details of ISO 27001:2013 model can be found at https://www.iso.org/standard/54534.html.

The Health Insurance Portability and Accountability Act (HIPPA) of 1996 was endorsed by the United States Congress in 1996. It has been known as the Kennedy–Kassebaum Act or Kassebaum–Kennedy Act after two of its leading sponsors.
This Act consists of 5 Titles. **Electronic Transaction and Code Sets Standards**, **Privacy Rule,** Security **Rule**,

National Identifier Requirements and Enforcement Rule for securing the patient ‘s digital data.

COBIT stands for Control Objectives for Information and Related Technology It is a security framework created by the ISACA (Information Systems Audit and Control Association) for IT governance and management. It supports managers in balancing technical issues, business risks and control requirements ensuring quality, control and reliability of information systems in organization.

Cyber Laws in India are enforced by the Ministry of Electronics & Information Technology(MeitY), Govt. of India. It provides legal recognition to electronic documents and a framework to support e-filing and e-commerce transactions and also provides a legal framework to mitigate, check cybercrimes.
You can follow given links to access the cyber laws mentioned in IT act.

Thank You!