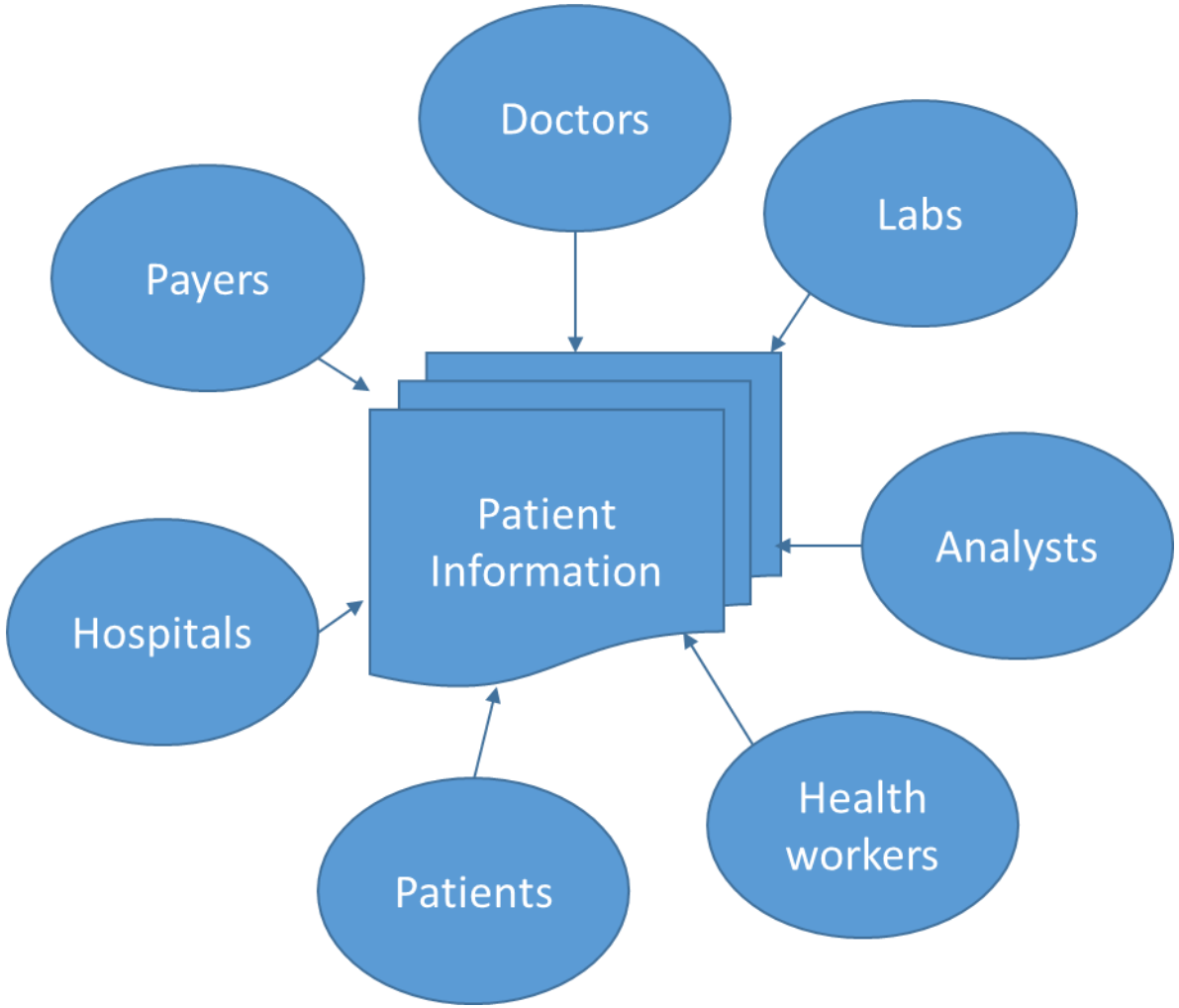
Data Security Standards and Requirements

National Resource Centre for EHR Standards (NRCeS)
C-DAC Pune

Healthcare Security

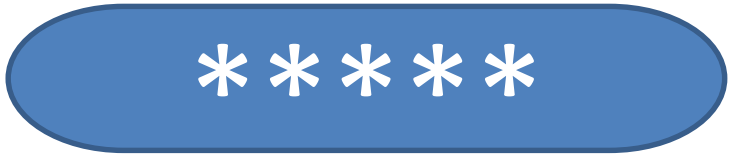
- Healthcare Security is complex & involves
  - Data of varied format, type, and size which is sensitive health information
  - Stakeholders with varied need and purposes to access health information

Appropriate preventive measures should be in place to ensure the confidentiality, integrity, and availability of all Health Information



Key Aspects of Data/Information

Confidentiality



Integrity

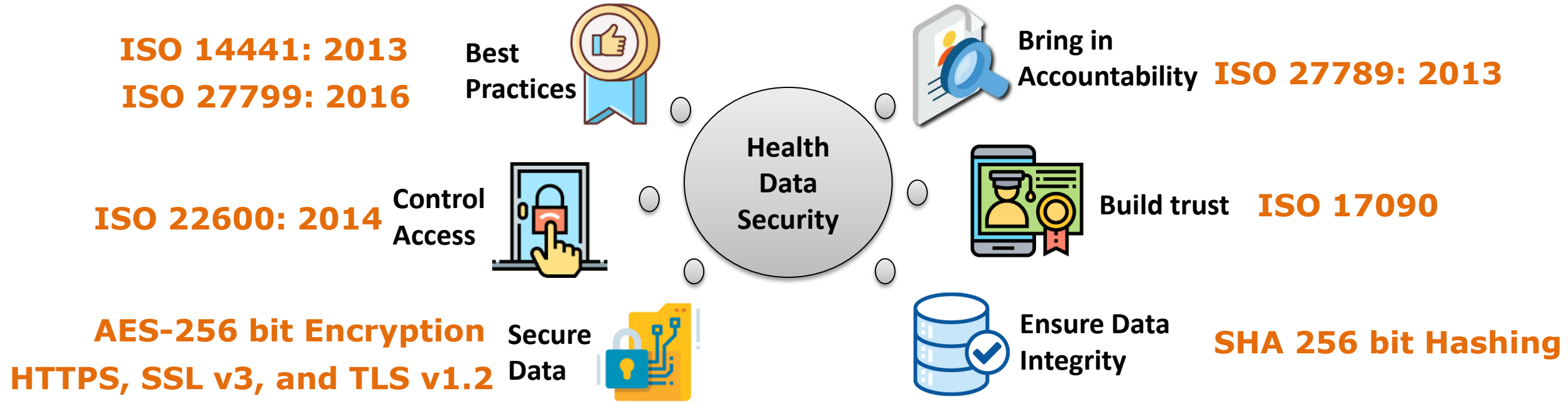
Availability

Need of Health Data Security Standards

- Protect against threats or hazards to the security or integrity of EHR
- Protect against unauthorized access of EHR
- Improve the quality of care by without infringing the privacy of the patient
- Address legal and ethical aspects in the digital healthcare scenario

Standards are a harmonizing force that helps increase the effectiveness

Health Data Security Standards



Health Informatics - Security & Privacy Requirements of EHR Systems for Use in Conformity Assessment

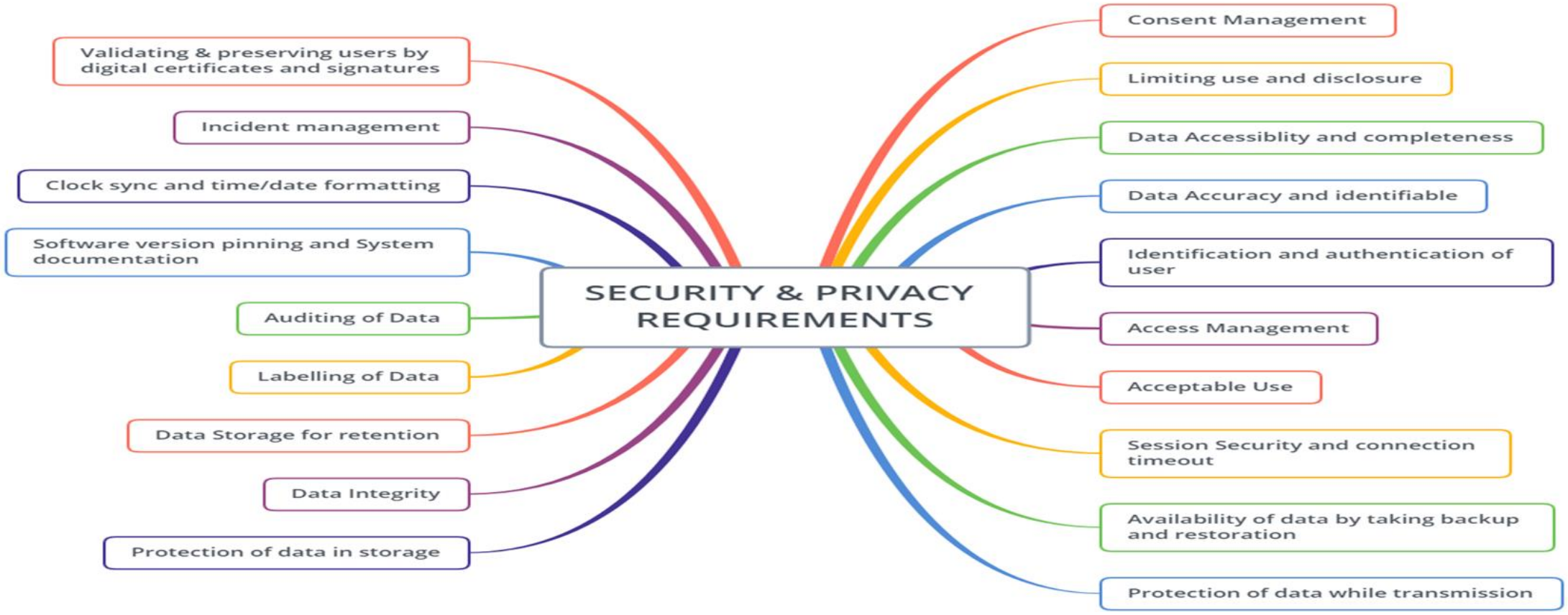
ISO/TS 14441:2013

ISO/TS 14441

- ISO/TS 14441:2013 Health informatics — Security and privacy requirements of EHR systems for use in conformity assessment
- Specification identifies the security and privacy requirements, which should be in place for conformance testing for interoperable Point-of-Service (POS) clinical systems interfacing with EHRs
- Privacy and Security Requirements
  - Covers 82 privacy and security requirements divided in 19 classes
- Conformity Assessment
  - Briefs about principles, approaches and considerations involved in conformity assessment
  - Conformity assessment processes and scheme

ISO/TS 14441: Privacy and Security requirements

There are total 82 privacy and security requirements which are classified into 19 classes, which are given as;



Consent Management

- Covers recording of consent, minimum data recorded, emergency access, logging emergency access, consent given by legally authorized representative, reporting changes to consent.

Example:

- Consent for new data entry
- disclosure of data
- transfer of data and its tracking details

Limiting use and disclosure

- Covers recording and storing only that data which has an identified purpose, restricting data exports, limiting disclosure of data subject's information to healthcare providers.

Example:

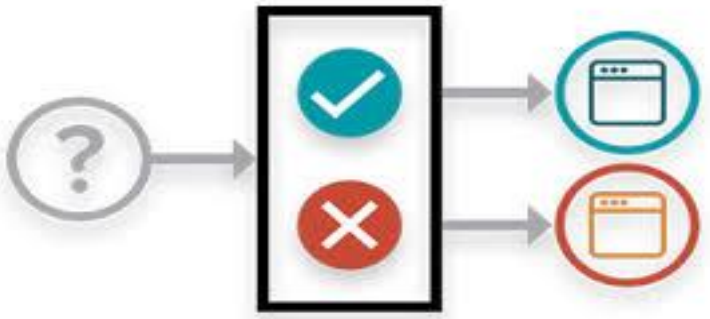
  - Data Recording
  - Data Storing
  - Restriction on data exports

Identification and Authentication

- Covers requirements for user identification, user and system authentication, authentication methods, protecting user profiles, passwords, and other authentication tokens, failed login attempts, user feedback during authentication.

Example:

  - User Identity
  - Privileges to user
  - Management of passwords, tokens, and user profiles



Access management

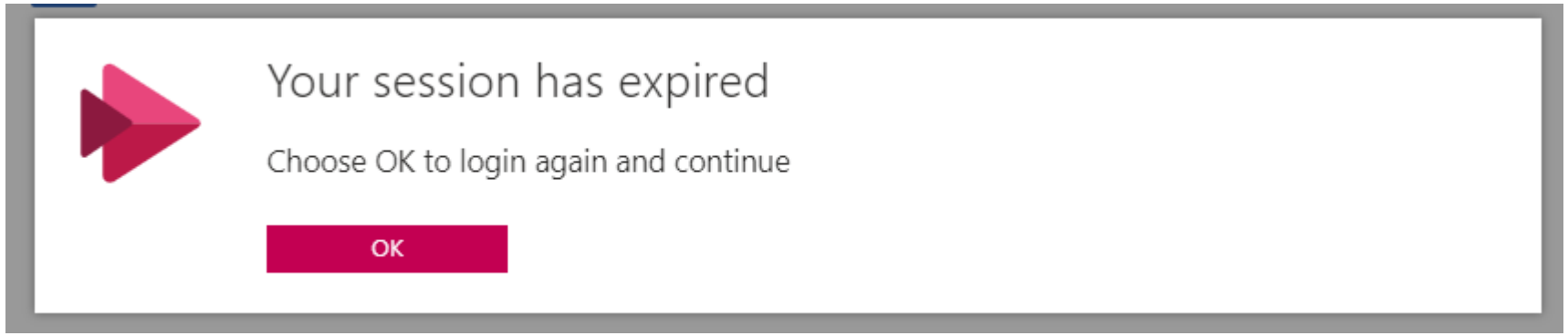
- Covers requirements for access controls, authorization control, role-based access control, delegation of access to the personal health information, reporting & restriction on access privileges, and also on revoking access privileges.

Example:

- Control over authoritative powers.
- Control over privileges usage.

Session security and connection timeout

- Covers requirements for session security, user session timeout, connection timeout, session security.



Availability of data by taking backup and restoration

- Covers requirements for backup, concurrent backup, restoration, reconstructing the content of an electronic health record at prior point in time.

Example:

- Replication of data
- Restore data

Protection of data while transmission

- Covers requirements for securing data during transmission, confirmation of data delivery,

Example:

  - Encryption using Public Key Infrastructure
  - Hashing algorithms
  - Notification on delivery confirmation

Health informatics - Information Security Management in Health using ISO/IEC 27002

ISO/DIS 27799

Background

ISO 27000 – Overview and Vocabulary

- Introduction to ISMS; terms and definitions

ISO 27001 – ISMS Requirements

- Formal specifications for an ISMS for certification

ISO 27002 – Guidelines for Information Security Management

- Guidelines for implementation of ISMS

ISO 27799 – Guidelines for Health ISMS

- Guidelines implementing and maintaining an ISMS in health-related organizations

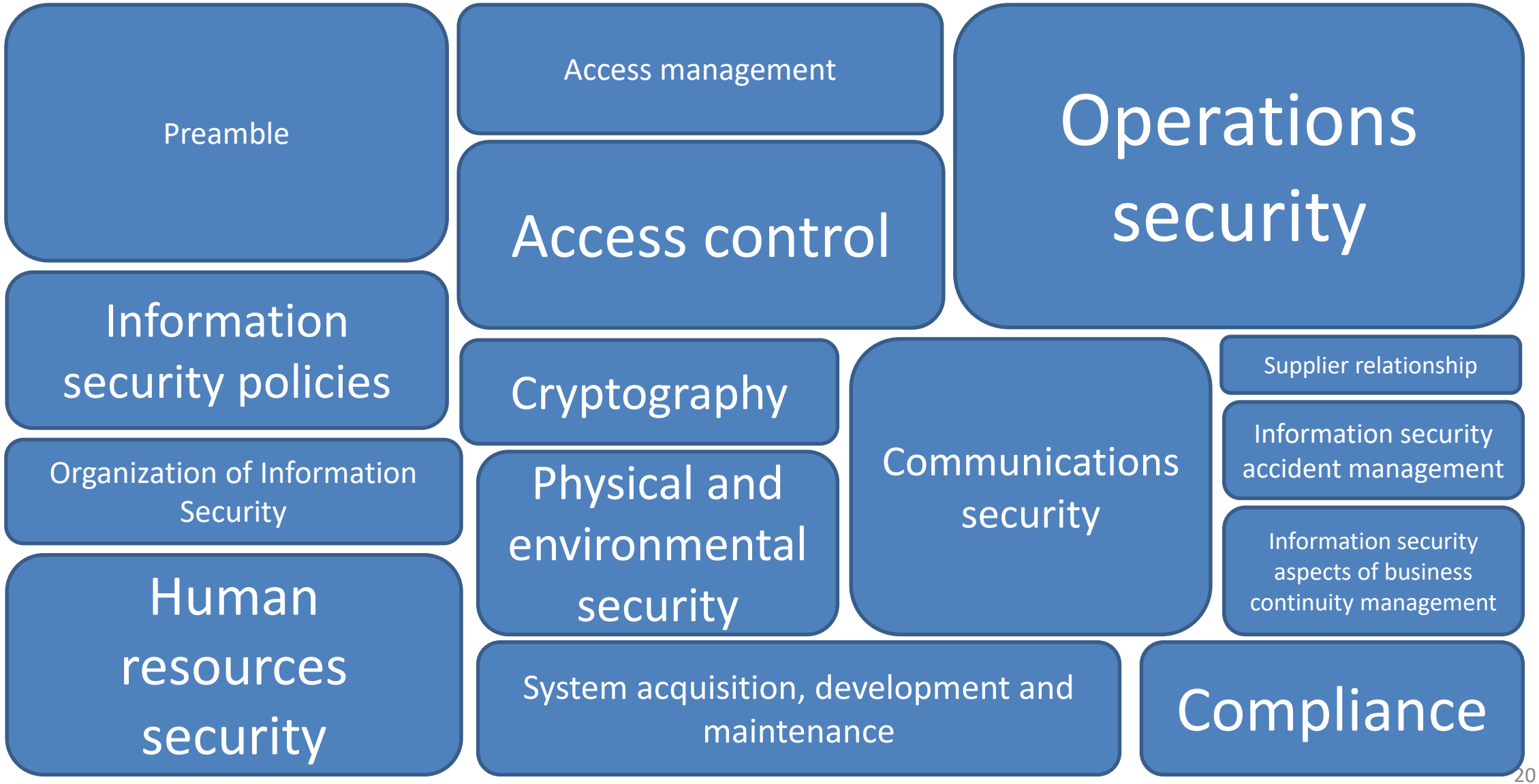
Terms and Keywords

Asset	Attack	Business Continuity	Control	Corrective Action
Information Asset	IS Event	IS Incident	ISMS	Threat
	Risk	Vulnerability	Statement of Applicability	

ISO/IEC 27002

- ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security controls
- Serves as a guideline for organizational information security standards and best practices for information security management
- It is meant to be used as a guide for identifying appropriate security controls within the process of implementing an ISMS
- Does not distinguish between controls applicable to your particular organization, and those which are not
- Defines the objectives and responsibilities of management.

ISO/IEC 27002 Standard Coverage



ISO 27799:2016

- ISO 27799 Health informatics — Information security management in health using ISO/IEC 27002
- It defines guidelines to support the interpretation and implementation of ISO/IEC 27002 in health informatics
- Standard for protecting Personal Health Information
- Adaptable to the wide range of sizes, locations, model of service delivery applications.

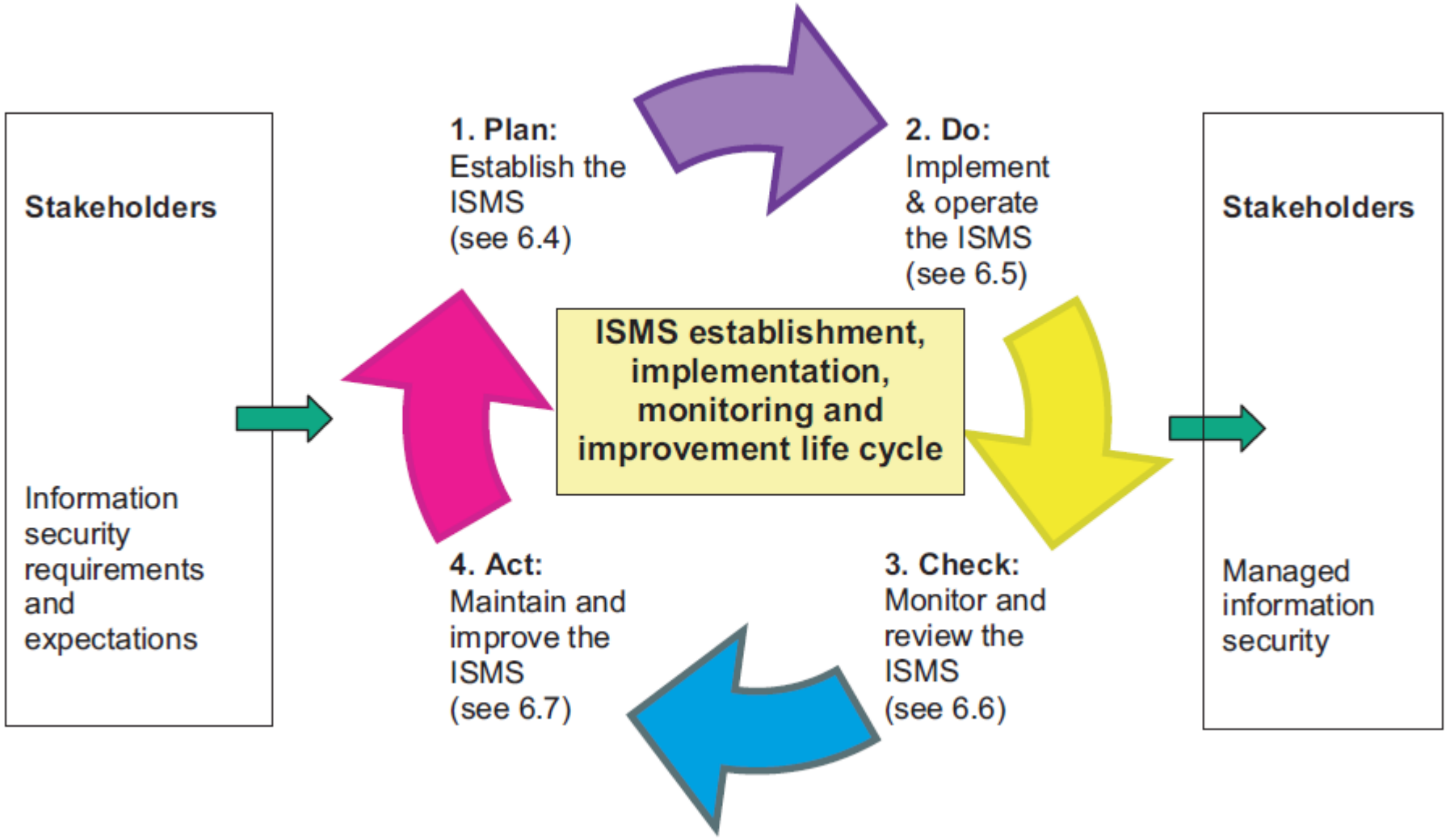
ISO 27799 – Health Information to be protected

- Personal health information;
- Pseudonymized data derived from personal health information
- Statistical and research data, including anonymized data
- Clinical/medical knowledge not related to any specific subjects of care (e.g. data on adverse drug reactions);
- Data on health professionals, staff and volunteers;
- Information related to public health surveillance;
- Audit trail data, produced by health information systems
- System security data for health information systems, including access control data and other security related system configuration data for health information systems.

ISO 27799 – Definition of PHI

- Personal Health Information
  - Demographic details
  - Financial and insurance details
  - Patient Identifiable information
  - Health records (including information derived form test/observations)
  - Patient’s treating healthcare provider identification

ISO 27799 : ISMS process overview



ISO 27799: Threats in Healthcare

- List of specific threats for healthcare environment
  - Theft by insiders/service providers/outsiders
  - Unauthorized use of a health information application
  - Introduction of damaging or disruptive software
  - Repudiation
  - Accidental misrouting
  - Technical failure of the host, system, storage facility or network infrastructure
  - Application software failure
  - Operator error
  - Staff shortage
- The consequences of these threats can be disastrous

Health informatics - Privilege Management and Access Control (Part 1 through 3)

ISO 22600:2014

Background

- Distributed availability of healthcare data
- Large EHRs are usually handled by distributed computing systems
- Traditional access control mechanisms may not work
- Advanced solutions for privilege management and access control are required
- The standard provides a policy-based access control framework for managing access control in distributed systems

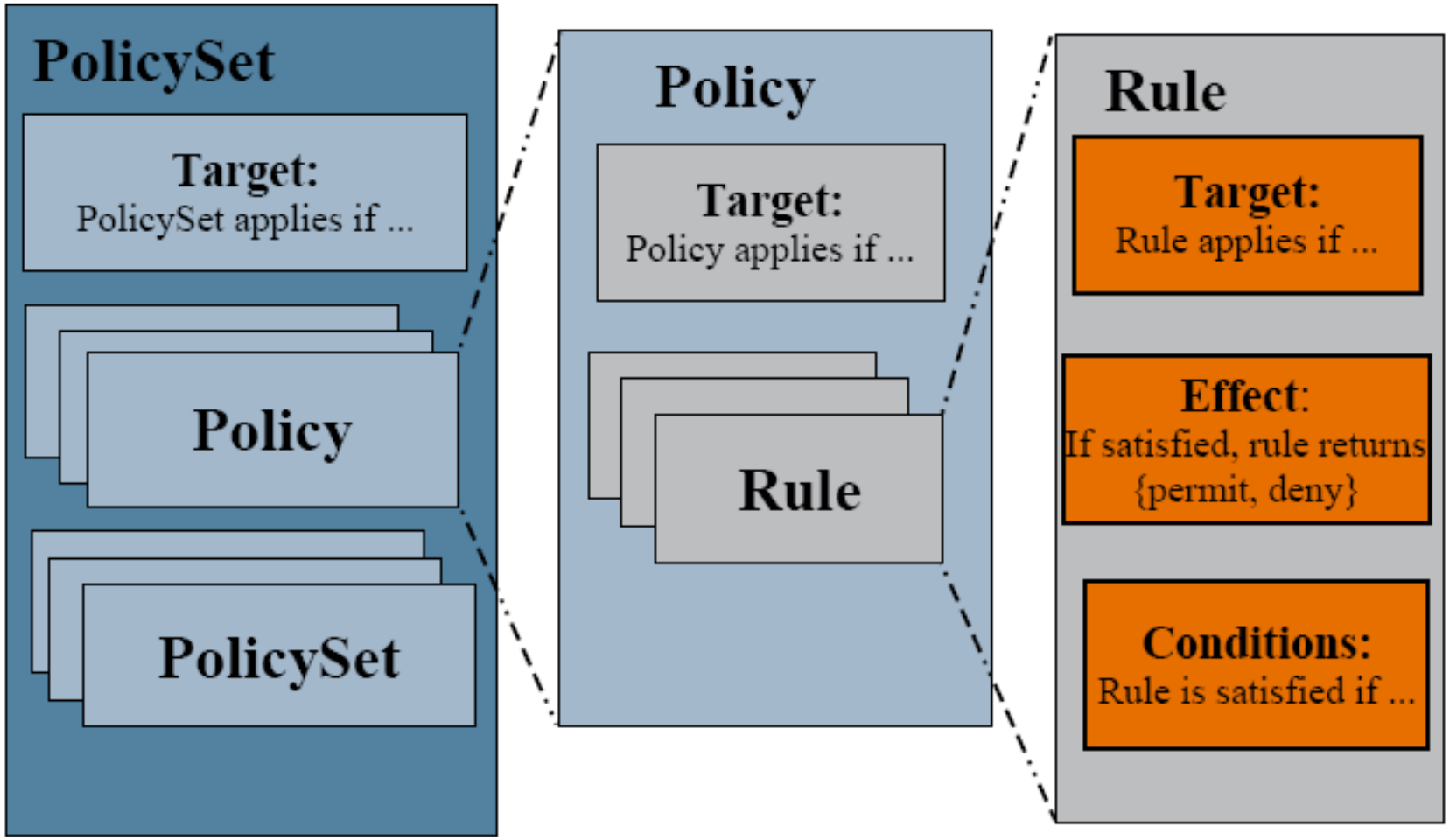
ISO 22600

- ISO 22600: Health informatics - Privilege Management and Access Control (Part 1 through 3)
- Part 1: Overview and policy management
  - Describes the scenarios of information exchange and basics of policy agreement
- Part 2: Formal models
  - Introduces models for architectural components and structure of Policies
- Part 3: Implementations
  - Provides implementation examples of the formal models
  - Describes application security services and infrastructural services using various specification languages (XACML, SAML)

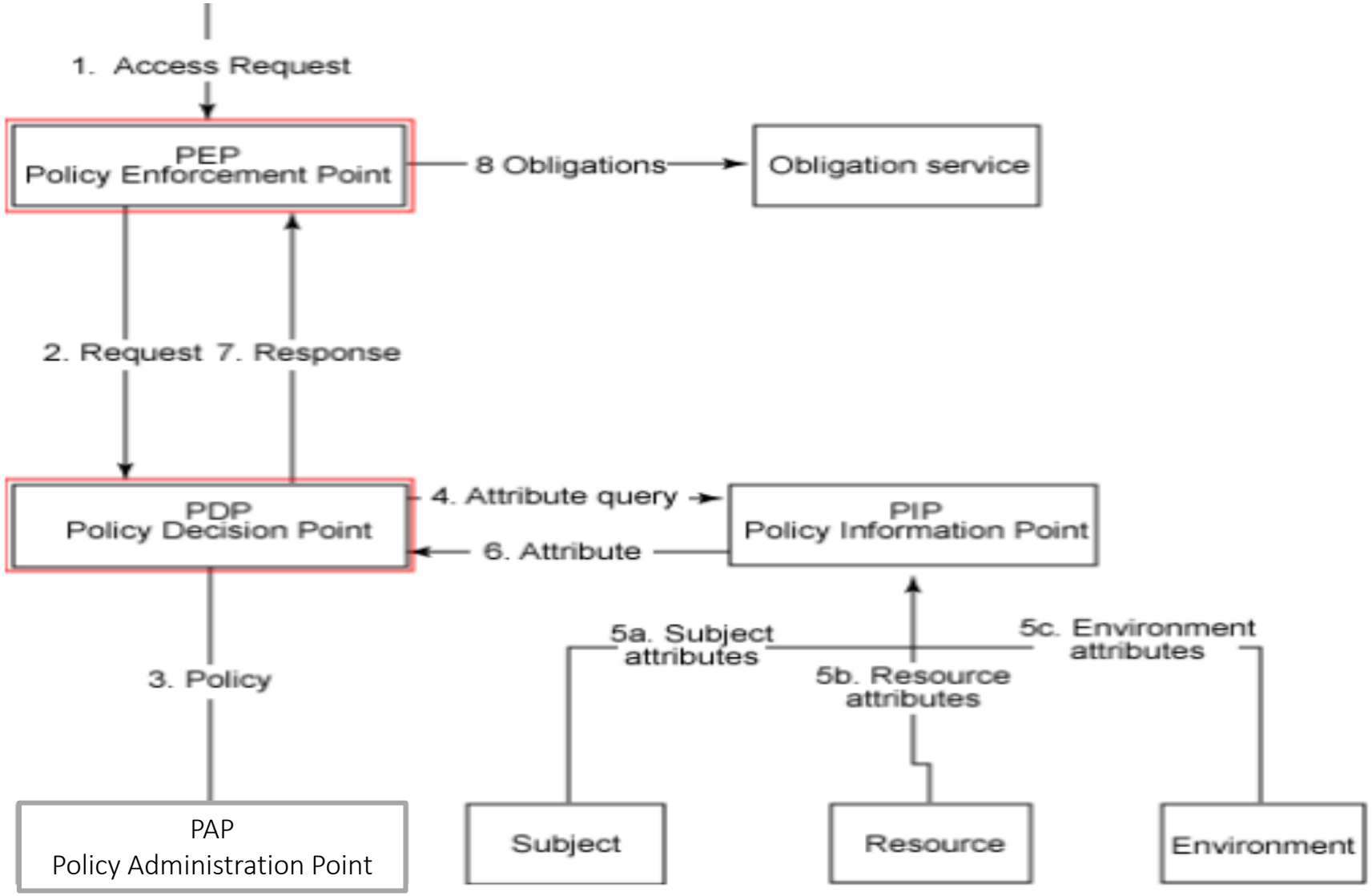
Structure of privilege management and access control

The structure consists of the following elements:

ISO 22600: Policy Structure



Example Architecture and Workflow



Example Policy

Physicians may read patient files for the purpose of diagnosis

```
<Policy  PolicyId="rule-centric-privacy"  RuleCombiningAlgId="permit-overrides">
    <Target/>
    <Rule RuleId="deny-all" Effect="Deny" />
    <Rule RuleId="matching-purpose" Effect="Permit">
      <Target>
        <Subjects>
          <Subject>
            <SubjectMatch MatchId="function:string-equal">
              <AttributeValue DataType="string">Physician</AttributeValue>
              <SubjectAttributeDesignator AttributeId="subject:role" DataType="string"/>
            </SubjectMatch>
          </Subject>
        </Subjects>
        <Resources>
          <Resource>
            <ResourceMatch  MatchId="string-equal">
              <AttributeValue DataType="string">PatientFile</AttributeValue>
              <ResourceAttributeDesignator AttributeId="resource:type" DataType="string"/>
            </ResourceMatch>
          </Resource>
        </Resources>
        <Actions>
          <Action>
            <ActionMatch MatchId="function:string-equal">
              <AttributeValue  DataType="string">Read</AttributeValue>
              <ActionAttributeDesignator  AttributeId="action-id"  DataType="string"/>
            </ActionMatch>
            <ActionMatch MatchId="function:string-equal">
              <AttributeValue DataType="string">Diagnosis</AttributeValue>
              <ActionAttributeDesignator AttributeId="action:purpose" DataType="string"/>
            </ActionMatch>
          </Action>
        </Actions>
    </Target>
  </Rule>
</Policy>
```

Implementation Aspects

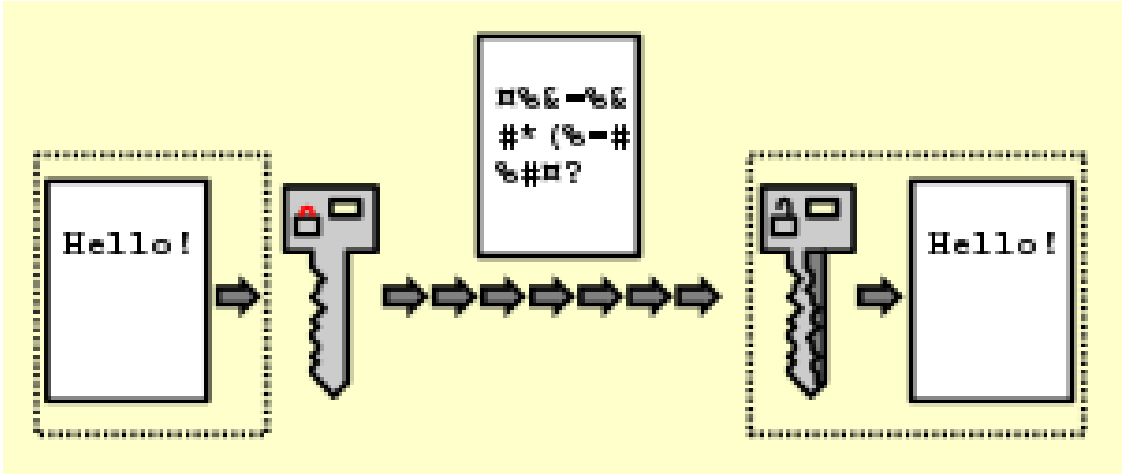
- Advisory standard for policy-based access control
  - Access control mechanisms such as Role Based, Policy Based, or singular user (applicable in case of mobile based PHR) are acceptable as long as conformant to applicable data security law(s) and rules as well as policy of the organization where implemented.
- Various access control mechanisms are applicable : Role Based, Policy Based, or singular user

Data at rest: Minimum 256-bits key length and Data at rest: HTTPS, SSL v3.0, and TLS v1.2

DATA ENCRYPTION

Data Encryption

- Way of scrambling data so that only authorized parties can understand the information
- Process of converting human-readable data to incomprehensible text, also known as ciphertext
- Requires the use of a cryptographic key: a set of mathematical values that both the sender and the recipient of an encrypted message agree on
- Securing PHI and keeping it confidential



Data Encryption

- Recommended encryption is minimum 256-bits
- Suggested Advanced Encryption Standard algorithm (AES) for encryption-decryption
- During data exchange Secure Transmission standards and mechanisms must be used HTTPS - HTTP over TLS v1.2 (formerly SSL)

AES Implementations

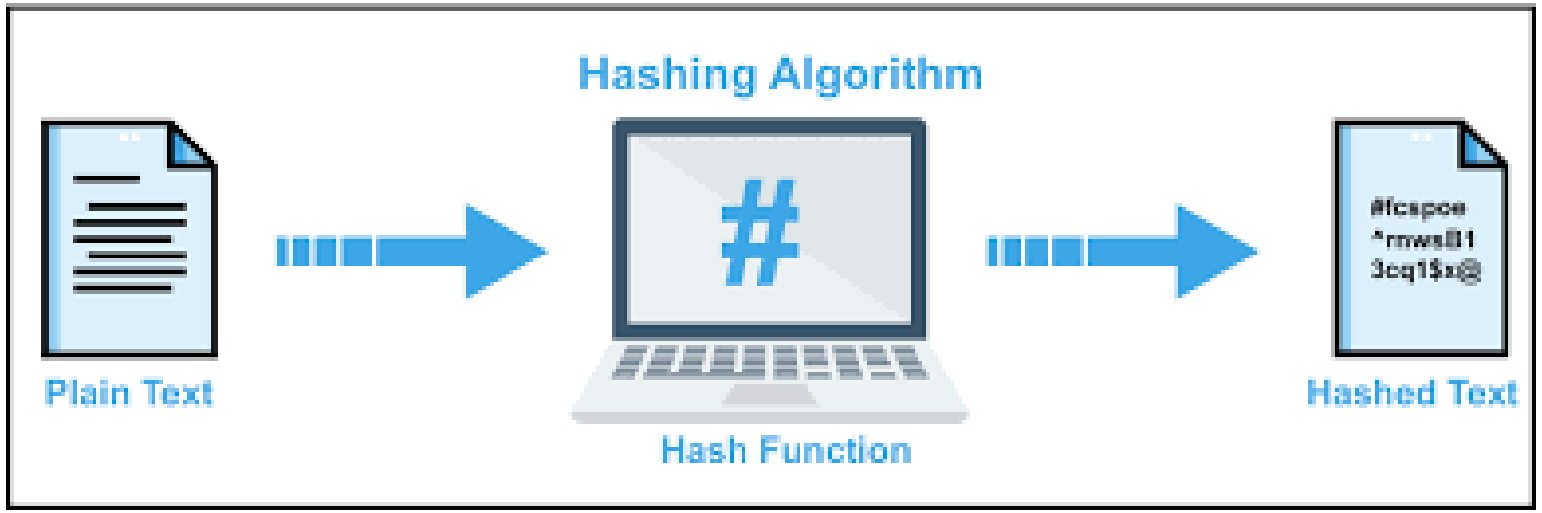
- C++ library
  - Botan has implemented Rijndael since its very first release in 2001
  - Crypto++ A comprehensive C++ public-domain implementation of encryption and hash algorithms. FIPS validated
- C# /.NET
  - As of version 3.5 of the .NET Framework, the System.Security.Cryptography namespace contains both a fully managed implementation of AES and a managed wrapper around the CAPI AES implementation.
  - Bouncy Castle Crypto Library
- Java
  - Java Cryptography Extension, integrated in the Java Runtime Environment since version 1.4.2
  - IAIK JCE
  - Bouncy Castle Crypto Library
- Python
  - PyCrypto – The Python Cryptography Toolkit PyCrypto, extended in PyCryptoDome
  - keyczar – Cryptography Toolkit keyczar
  - M2Crypto – M2Crypto is the most complete OpenSSL wrapper for Python.
  - Cryptography – Python library which exposes cryptographic recipes and primitives.
  - PyNaCl – Python binding for libSodium (NaCl)

Secure Hash Algorithm (SHA) used must be SHA-256 or higher

DATA INTEGRITY

Hashing

- Way to ensure data integrity and authenticity
- A unidirectional process
- Hash value can be considered the summary of everything of data/file
- A hash is usually a hexadecimal string of several characters



- Recommended Secure Hash Algorithm (SHA) SHA-256 or higher

Implementations

- Password hashing
  - Verify the integrity of your password
- EHR Data Masking/ de-identification
  - sets of alterations and changes made to PHI
- Medical record Reliability Verification
  - PHI Integrity check
  - Digital Certificates
- Large-scale search and pattern matching, exhaustive comparison
  - Medical Image Searches

Health informatics - Public Key Infrastructure (Part 1 through 5)

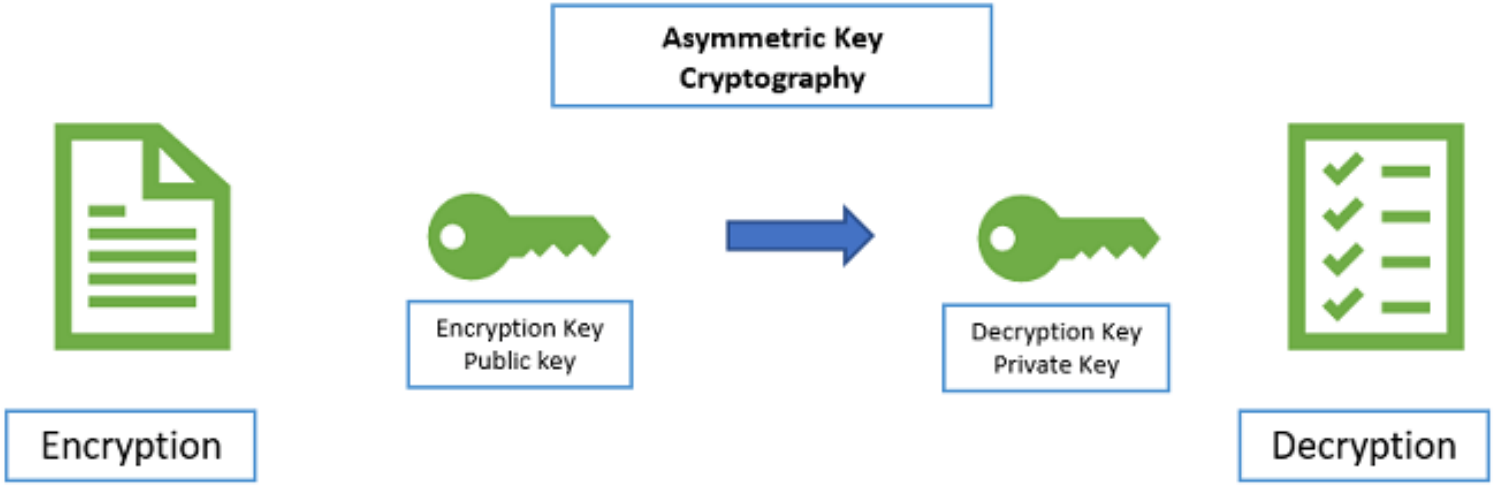
ISO 17090

ISO 17090

- ISO 17090 : Health informatics - Public Key Infrastructure
  - Part 1: Overview of digital certificate services
  - Part 2: Certificate profile
  - Part 3: Policy management of certification authority
  - Part 4: Digital Signatures for healthcare documents
  - Part 5: Authentication using Healthcare PKI credentials
- PKI in health is a critical part because the certificate-based technology helps healthcare organizations establish trusted signature, encryption, and identity between people and systems

ISO 17090: Terms and Entities

- Public Key Infrastructure (PKI)
- Digital Certificate
- Certificate Authority (CA)
- Digital Signature



Potential uses of digital signatures in healthcare

- Medical Certificates
- Treatment prescriptions (ePrescription)
- Reimbursement Applications
- Medical examination attestation

Without digital certificates: As signature of these documents is required by law or administration, paper documents are printed and signed by the authorized persons and sent by postal services

With digital certificates: The public and private keys and certificates for the signature will be distributed to each doctor. The sender or author signs the whole bundle [document(s) plus attribute certificates] using signature key. The receiver can verify the integrity and authenticity of the document using sender's public key.

Health informatics - Audit trails for Electronic Health Records

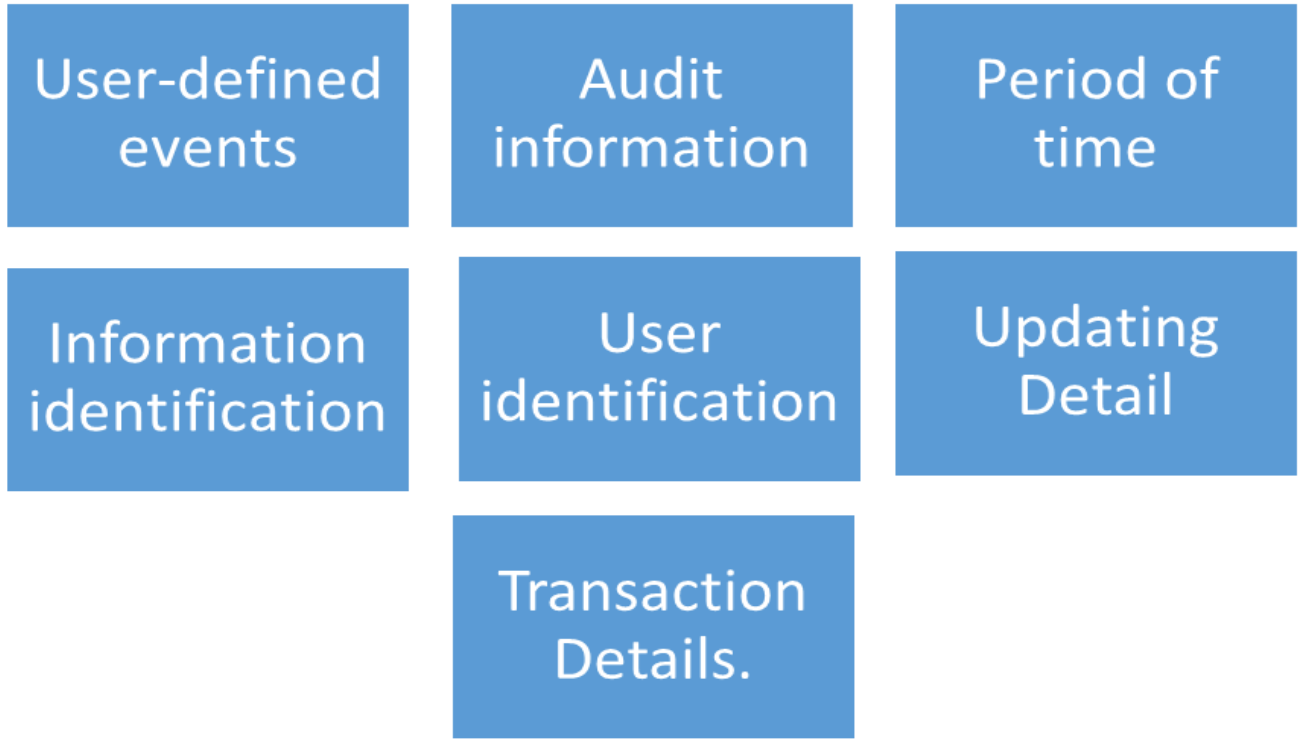
ISO 27789:2013

ISO 27789:2013

- ISO 27789:2013 Health informatics — Audit trails for electronic health records
- Audit logging helps to ensure accountability
- Goals:
  - Information captured in an audit log is sufficient to clearly reconstruct a detailed chronology of the events that have shaped the content of an electronic health record
  - An audit trail of actions relating to patient's record can be reliably followed, even across organizational domains.

Audit Trails and Logs

- All actions related to electronic health information including viewing should be recorded



Implementation Aspects

- IETF RFC 3881 – Defined the Information Model
- HL7 FHIR Audit Event Resource
- DICOM Audit Message Schema (derived from IETF RFC 3881)
- DICOM Audit Log Message – Made the information model Normative, defined Vocabulary, Transport Binding, and Schema

SUMMARY

Applicability of Security Standards

- The applicability of few security standards such as Privilege management and Information Security Management depends upon:
  - Application's Functionality, size, complexity, and capabilities
- All the set standards for data encryption, communication, non-repudiation, integrity and others are applicable to all the healthcare applications which are generating and exchanging health information
- Other security management and standard / practices / guidelines given by Law – (IT Act 2000 and amendments) or regulatory / statutory / certification bodies i.e. NHA, NABH))

Thank You

nrc-help@cdac.in