# HCISPP Requirements

2 years in Healthcare IT security. 3 hour exam and 125 multiple choice questions with a 70% minimum passing score.

# HCISPP Domains

1. Healthcare Industry - 12%
2. Information Governance in Healthcare - 5%
3. Information Technologies in Healthcare - 8%
4. Regulatory and Standards Environment - 15%
5. Privacy and Security in Healthcare - 25%
6. Risk Management & Risk Assessment - 20%
7. 3rd party risk management - 15%

# Organizations in Healthcare

## Patients

Someone currently receiving care.

Inpatient - admitted for 24hr or more

Outpatient - 24hr or less

Has PHI and PII to protect

PHI and medical history hard to correct once altered

## Providers

Single entity (Nurse, physician, therapist) or Organization (hospital, clinic, & virtual healthcare providers) that provides a medical service

Integrated Delivery Systems - organizations that support both inpatient and outpatient

### Physicians

Diagnose and treat the patient

MDs, and DOs. Credentialed speciality specific to their practice: cardiologist, endocrinologist, neurologist, oncologist, pathologist, OBGYN, surgeon, plastic surgeon, psychiatrist, urologist

Requires medical school and intern + residency

### Physicians Assistant

Goes to PA school

Works under physician and can do most except perform surgery

### Medical Technician

Operates and maintains medical device or operates in clinical laboratory setting

But Diagnosis and interpretation are left to Physician

Includes biomed techs and clinical engineer

### Other Medical

Nurse, nurse’s aid, registered nurses (RN/CRNA/CNM), nurse practitioner (NP), licensed practical nurse (LPN)

### Administrators & environmental services

Admins can include finance, IT, information security, chief data officer

Environmental services can be housekeeping and janitorial

### Other Personnel

Business partner - provides similar service

Business associate - provides different service ex: MSSP

CHO - community healthcare organization

## Payers

Includes all Healthcare insurance providers

Indemnity Insurance vs Employer-based insurance provider

Employer-based can be fully insured plan or self funded employee health benefit plan

## Healthcare Clearinghouse

Interprets claim data between providers and insurers. Clearing houses are a contracted vendor who reformats the claim into HIPAA transaction format and digitally forwards to third party payer.

## Medical Coding and classification systems

* Medical coding is a set of International standards for billing and payments that is universally accepted (private & government)

Doctor Narrative is categorized as unstructured

DRGS - classification for common diagnosis (prospective payment system of inpatient services)

ICD-10 - classification of diseases and related health problems. Explains why a patient needs healthcare services. Most accepted (ICD-9 is old, ICD-11 coming, inpatient mostly)

SNOMED CT - terminology framework used to describe clinical terminology. Works with ICD

### Additional coding systems

LOINC (logical observation Identifier names and codes) - lab/clinic observations

APG (Ambulatory Patient Group) - classifies outpatient services reimbursement

APC (Ambulatory Payment Classification) - medical reimbursement

RUG (resource utilization groups) - long term care insurance billing

CPT (current procedural terminology) - classify services provided for reimbursement purposes. Explain what the physician did for the patient.

CDT - dental coding

NDC (national drug code) - directory for identifying (but not evaluating) drugs

HCPCS Level II (healthcare common procedure coding) - US gov. similar to ICD but for outpatient & gov.

DSM - mental disorders

ICF (international classification of functioning)- reporting disabilities

Coding -> Billing -> reimbursement

## Revenue

Claims typically require pre approval.

### Payment Models

fee for service - pay for care episodes, therapy, or the service

Capitation - fixed predetermined amount agreed by provider, whether the patient sees provider for care or not

Salary - ex hospitals w shared offices

US uses fee-for-service models:

PCMH - primary care manager coordinates treatment for patient

ACO - contract between willing coalition to provide broad set of care to patient (fee-for-service)

### Billing

EOB - explanation of Benefits (to patient)

ERA - electronic remittance advice. For several patients (to provider), to explain payments

Co- payment - set & standard fee

Deductible - annual out of pocket amount before coverage

Co-insurance - ex: 80/20 or 70/30. A percentage between patient and 3rd party

* Claims can be denied for not being a medical necessity and notified via those docs
* Claims rejected for incorrect codes

HIPAA Transaction & Code Sets (TCS) - rules for exchange of healthcare information. Uses CPT for procedure codes and uses ICD for diagnoses.

A SC X12N Claim Protocol - ANSI HIPAA protocol. Uses x12 xml schemas for TCS

National Uniform Billing Committee (NUBC) - standaaw rdized billing

Separation of duties - not 1 person responsible for all phases of a transaction. Restrict fraud.

EHR - electronic health record. Intended use for doctors.

PHR - personal health record. For preventative health controls and personal devices. Ex: what you eat or blood pressure. Can link with EHR.

NHN - national healthcare network

HIT - health information technology or the electronic systems that health care professionals – and increasingly, patients – use to store, share, and analyze health information

* Hardware (medical device), software, or interoperability (HIE)

HIE - health information exchange to appropriately access and securely share a patient's vital medical information electronically. improves quality and safety of patient care providing Interoperability + security

* HIE is an example of HIT
* Interoperability: EHRs are maintained by individual physicians and organizations
* Security: reduce fraud and abuse
* Provides feedback from actual practice to research
* Provides backbone of technical infrastructure for national and state-level

Privacy

* Minimum necessary use: ensures minimal and appropriate access
* Audit logs: for detection of access violation

Safety

* Data integrity checks
* Availability checks

### Standards

NIST frameworks are optional for healthcare in US

HIPAA Identifies

1. Health Plans
2. Providers of services
3. Health information clearinghouses
4. Business Associates (ex: subcontractors)
   1. Org responsible for associates use of data

U.S. HIPAA Privacy Rule

* Safe Harbor for limited data sets: Patient data, or limited data set, can be used for research without consent if 18 De-identifying requirements are met or expert has determined
* Applies to physical/verbal matters
* Therapist notes are example of privacy data

U.S. HIPAA Security Rule

* Applies to electronic transmissions

HITECH

* Enhances HIPAA by declaring HHS Office of Civil Rights as enforcer of HIPAA privacy and security rules
* Provides specificity about the adoption of EHRs

ISO 27001

Focused on Information Security Management System (ISMS) aka the governance supporting infosec program. Can get 27001 certified.

1. Reqs of ISMS
2. Management responsibility
3. Internal ISMS audit
4. Management review of ISMS
5. ISMS improvement

ISO 27002

Provides “code of practice” for Infosec management. Used with 27001.

Control Objectives:

1. Security Policy
   1. Provides management guidance and support for infosec
2. Organization and Information Security
   1. Formal security mechanism in org
3. Asset management
4. Human Resources security
5. Physical and environmental security
6. Communications and operations management
7. Access control
8. Information system acquisition, development and maintenance
9. Information security incident management
10. Business continuity management
11. Compliance

Leaders must act on known risks!

### Policy

#### Taxonomy

Laws -> General Organizational Policy (security statement) -> Functional Implementing Policies (security directive) -> standards, procedures, baselines

#### Writing security policy

* Policy should survive up to 5 years
* Policy creation and maintenance is defined
* Don’t be too specific or include technical implementation details
* Directive wording and keep short
* Review w management sign off and employees acknowledging
* Adjust policies based on periodic review of policies or incidents

#### Policy types

* Organizational
  + Management or program level
* Functional (issues specific)
  + Ex: internet browsing or email use
* System specific

## Workflow Management

Provider processes. Often automated with sensitive data and legacy systems.

Store, Access, manage, share

### Clinical Workflow

EDI - electronic data interchange. Language or standard for transactions. Sensitive data.

HCFAC - agency for fraud and abuse prevention

### Breach Rules

Breaches can lead to attacker using victims medical services and therefore an erroneous EHR that can cause adverse medical outcomes.

Breaches most likely to happen in the “dispose” information lifecycle phase

HIPAA

* mandatory breach rule
* Safe harbor provision for encrypted information

HITECH Breach Rule

* Notify individuals within 60 days
* Report breaches of 500 or more to HHS Office of civil rights promptly (60 days)
* Report less than 500 annually
* Mail letters of breach. Post on the org’s website if 10 letters are returned to the sender.
* Conduct risk assessment after breach
* Safe harbor provision for encrypted information not having to be reported as breach
  + Must be FIPS 140-2
* $1.5M fine

States and local govt have breach rules too

Healthcare Records Management

* responsible for filing, storage, retention schedule, destruction, etc

Vendors - Business associates with relationship with healthcare facility (ISP, AWS, IR)

CMS - center for Medicare and Medicaid. Federal.

AMA - American medical association. Private.

Joint commission - provides accreditation for a provider organization

## Roles in Regulatory Environment

* Data owners: defines metrics for data and collects the data (ex: lab tech)
* Data controllers: responsible for management of data
* Data custodians: determine access control to the data (ex: IT)
* Data processors: processes data but not responsible for data
* Data steward: governance role to ensure quality of data
* Data protection commissioner (DPC)

Regulators

DHHS (dept of health and human services), OCR (office of civil rights), NIST, FIPS, FTC, EC (Europe), CNIL(France), ICO(uk), HSE (Ireland)

RHIOs - regional health information organizations

ARRA - American recovery and reinvestment act

NISD - network and information security directive (UK)

NCSC - National Cyber Security Centre

### Information Flow Mapping/Models

* State machine model: one point in time
* Multilevel lattice model: strict layers of subjects and objects
* Noninterference Model: limit higher classified info shared with lower privileged
  + Ex: Bell-LaPadula where subjects can read information from objects at some of the classification levels or lower levels
* Matrix based models: one-to-one relationships
* Information flow models: data allowed or not allowed between objects
* Biba integrity model: subject prevented from reading less accurate (or with integrity) objects but can read objects more accurate
* Brewer-Nash: subject has access to objects with sensitive information associated with two competing parties to prevent conflict of interest

### HMO vs PPO vs POS

HMO - health management organization. HMO align with providers in agreement to give care to patients.

PPO - preferred provider organization accessible with a fee-for-service health plan.

POS - point of service. Combines HMO and PPO.

### Health Data Classification

Based on risk management and compliance

NIP - national provider identifier

Healthcare provider taxonomy code:

* level 1 - provider type
* Level 2 - classification
* Level 3 - specialization

### Data Exchange

HL7 - health level 7 - deals with layer 7 OSI transfer for ePHI

DICOM - HIPAA protected digital imaging communications

NIMIS - Ireland’s version of DICOM

IHE - integrating the healthcare enterprise - sharing ePHI between providers/orgs using ICTs

### Legal medical records

DRS (designated record set) - legal Records about individuals used by coverage entities to make decisions about care

# Regulatory Environment

Local and state laws to federal and international laws because of interoperability

HIPAA Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information

# Privacy and Security in Healthcare

## Information Security

C.I.A. Are the pillars

Hashes: one way function for Integrity of data.

* Good for preventing MitM attacks.
* MD5 is broken in 1996

Encryption for confidentiality. Symmetric vs Asymmetric

* Symmetric for bulk data. DES is broken.
* Hardware encryption. Ex: encrypted SSD or a TPM
* Software encryption. Ex: bitlocker and PGP

Digital signatures or HMAC for authenticity

Non-repudiation to prevent of denying actions

* Ex: a compromised shared password

Access Control

Should be Least privilege aka “minimum necessary” under HIPAA

* MAC: mandatory access control. Most restrictive; for govt. Decision made by central authority, not object owner. Matches subject label to object label. Example is lattice-based access control (LBAC. based on the upper and lower bounds interaction between any combination of objects and subjects)
* DAC: discretionary access control. Least restrictive (used in Windows & Unix). Based on object ownership and granting subjects access.
* RBAC: role based access control or non-discretionary. Central authority in an organization (ex: AD) that aligns permissions to granted roles
  + Rule based access control: flexible RBAC variant. Set rules to dictate the assignment of roles (decentralized authority. Usually governed by data custodians)

Authenticity

* Something you know
* Something you have
* Something you are

PKI - infrastructure for managing asymmetric keys. Digital signatures use PKI and asymmetric keys.

### Business Continuity

Per NIST 800-34 7 step process:

1. Develop the contingency plan policy statement
2. Conduct the business impact analysis (BIA)
   1. Impact of Critical processes and How quickly business must resume in terms of: maximum time down (MTD), recovery time objective (RTO) and recovery point objective (RPO)
3. Identify preventive controls
4. Create contingency strategies
5. Develop a information system contingency plan
   1. Supporting information (ex: plan’s scope)
   2. Activation of plan and notification of key individuals
   3. Recovery phase. How recovery will occur.
   4. Reconstitution phase. What needs to occur
   5. Appendices and additional plan detial
6. Ensure plan testing, training, and exercises
7. Ensure plan maintenance
   1. Update plan

## Privacy

“Separation of duties” - checks and balances in process to ensure minimum 2 people must collude to commit fraud or for fraud to happen

Privacy violations: Very old people (89+) can be de-identified due to fewer peers alive (although HIPAA has no age requirements). HIV positive patients don’t need their status disclosed to providers like dentists.

GINA or genetic non discrimination act. Prevents genetics used for hiring or insurance coverage.

### Logging

Logs can Include:

* User IDs
* Dates and times
* System identity (MAC, IP address, host-name)
* Successful and Rejected access attempts

Logs should be:

* retained for a specific period (org + regulatory)
* Access Protected
* Periodically reviewed by party other than log monitoring team

# Risk Management

## Governance Structure

Information owner/steward - business centric party that determines impact, cost, and access of info

Information system owner - a business area Ex: IT department

Information Systems Security Officer (ISSO) - implement security controls

End User - employee that transmits, stores, or deletes info

Risk Assessment Team to include staff across all business units

## NIST 800-39 Risk Management Methodology

1. Framing risk
   1. produce risk strategy, identify risk tolerance, assumptions, and constraints
2. Assessing risk
   1. Identify threats, vulnerabilities, impact, likelihood, and determine risk
3. Responding to risk
   1. Identify consistent response to risk from org-wide perspective
4. Monitoring risk
   1. Continuously

## Risk

Quantitative risk

* Measurable ex: Annual Loss Expectancy

Qualitative risk

* Descriptive “high, medium, low”

Financial Risk

* Can be transferred through insurance policy

Reputational risk

* can’t be “transferred”

Risk strategy - what organization is going to do regarding risk management

Risk processes - how organization will accomplish risk management

Risk Tolerance - compliance based. defined by senior leadership rather than the system owner or IT

### NIST 800-30 risk Assessment process outline

1. Prepare for assessment
2. Conduct risk assessment
3. Communicate results of assessment
4. Maintain assessment

ALE - annual loss expectancy

Vulnerability - weakness in system

Exposure - vulnerability that is used as stepping stone into network by a hacker

Threat - event with potential to adversely impact to organization

Threat sources

* Human (insider), environmental (bio waste), operational, natural (flood), technical (malicious code)

### Asset Valuation

Tangible asset Valuation - physical presence. Original value minus depreciation

Intangible asset valuation - non-physical ex: patents, IP, PHI

## Secure SDLC and Maturity Frameworks

[HSCC’s joint security plan (JSP)](https://healthsectorcouncil.org/the-joint-security-plan/)

## Controls

### Cybersecurity best practices

[HSCC’s Healthcare industry Cybersecurity Practices (HICP)](https://healthsectorcouncil.org/wp-content/uploads/2018/12/HICP-Main-508.pdf)

### Control Types

* Corrective
* Preventive
* Detective

HIPAA’s security safeguard rules state that controls can be:

* Administrative/managementEnforced through policies, procedures, standards, and guidance
  + Ex: security management program
* Operational
  + People or processes that use people
  + Physical controls are a type of operational control
* Technical
  + Software, hardware, and firmware

These controls types can be further refined and mapped to 18 NIST/ FIPS 200 control families

* Access control - technical
* Awareness training - operational
* Audit and accountability - technical
* Security assessment and authorization - management
* Configuration management - operational
* …..

### Incident Response Timeline Controls

* Directive
* Deterrent
* Preventive
* Compensating
* Detective
* Corrective
* Recovery

Compensating controls lead to residual risk

Risk Acceptance: who is responsible for the risk?

NIST 800-39 Multi-tired risk management process (strategic risk)

* Tier 1: organization
* Tier 2: mission / business processes
* Tier 3: information systems
* includes traceability and transparency of all risk based decisions

NIST 800-37 Risk Management Framework (RMF)

1. Categorize information system
   1. Architecture descriptions and organizational inputs
2. Select security controls
3. Implement security controls
4. Assess security controls
5. Authorize information system
6. Monitor security controls

## Other Risk Frameworks

ISO 27000 family - international standard for security management

ITIL - IT Infrastructure Library. 34 books by British govt

COBIT Framework - for high level control Objectives

CRAMM - CCTA Risk Analysis and Management Method (identify & valuation, vulnerability assessment, countermeasures selection)

FMEA - failure modes and effects Analysis (immediate or module level, intermediate or process level, system level)

FRAP - facilitated risk analysis processes. Prescreen to see if risk analysis is needed. Ideal for small organizations.

OCTAVE - operational risk and security practices focused risk Assessment

Spanning Tree Analysis - or attack tree

VAR - value at risk. Identify threats, estimate likelihood, estimate VAR, risk mitigation)

SOMAP Risk Assessment Workflow

* Data collection
* Threat analysis
* Vulnerability analysis
* Risk acceptance
* Risk treatment

Remediation/Corrective Action Plan or (CAP): what needs to be done? Ex: training, processes, controls, maintenance

Strategic Plans: high level business plan stating goals

Tactical Plan: initiative to support goals in strategic plan

Risk Treatment options:

* Mitigation
  + Address and eliminate the risk
* Transfer
  + Someone else’s problem
* Accept
  + Ex low risk & high cost to fix
* Avoid

Exception Handling: document exceptions. Describe in detail the duration, individual requesting, and additional risk from granting exception

### Risk Reporting Metrics

* The threat
* Risk (or likelihood/impact)
* Cost of safeguard
* Residual risk remaining
* Timeframe

KRI - key risk indicator - early signal for emerging risk

KPI - key performance indicator - alert for underperformance of an asset

# Information Risk Assessment

* Identify, estimate, and prioritize risks
* PHI has higher $$ value for criminals than PII
  + Fraudulent billing or free care for criminal
* During a breach, PHI has same impact regardless of form or where it is stored

Adverse Outcomes

* Financial loss
* Repudiation loss
* Regulatory/legal losses

Risk Assessment - identify infosec vulnerabilities, estimating value, and prioritizing

Continuous Threat Monitoring and Information Sharing Organizations

* Intelligence sources: H-ISAC, HITRUST C3, NCCIC, US-CERT, and CSIRT
* [HSCC’s matrix](https://healthsectorcouncil.org/hic-miso-pdf/) of information sharing organizations

HCISPP says external risk assessments are best because it’s an impartial reviewer. This is because Infosec and info steward personnel could want to hide issues

T.V.L.I. = threats \* vulnerabilities \* likelihood \* impact

* Determine impact on organization’s mission
* Determine cost of replacing information
* Determine who has a need for information & when
* Determine information destruction

## Tools and techniques

### NIST 800-30 Risk Assessment Process

Information system risk management

1. Identify and characterize Asset
   1. Aka Information gathering. Assets that org owns, accesses, or uses under contract including all 3rd party access
   2. Arguably most important as this determines control baselines, assessment methodology, and impact of system
2. Threat identification (history of attack, intelligence)
3. Vulnerability Identification (test results, audit comments, sec requirements)
4. Control (or countermeasure) analysis (based on planned and current controls)
5. Likelihood determination (current controls, threat motivation, threat capacity)
6. Impact Analysis (in terms of C.I.A.)
7. Risk determination (impact, likelihood, and controls)
8. Produce Control recommendations
9. Document results in risk Assessment report

### NIST 800-66 Risk Assessment Process

Written for implementation of HIPAA security rule. Dictates encryption of ePHI.

### HITRUST CSF

* Common Privacy and security framework for HIPAA and GDPR

### Assessment Tooling

Organizational level HIPAA risk Assessment tooling

* ONC’s [SRA Tool](https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool)
* HIMSS Risk Assessment Toolkit (discontinued?)

Application level:

* [HIMSS application security questionnaire](https://www.himss.org/application-security-questionnaire)
* [HIMSS cloud computing risk Assessment](https://www.himss.org/sites/hde/files/d7/HIMSSorg/Content/files/RA05_RA_Cloud_Computing.xlsx)

NHS Data security and protection Toolkit (previously IG Toolkit)

* an online self-assessment tool for UK orgs that allows organizations to measure their performance against the National Data Guardian’s 10 data security standards (27002, data protection act 1998, confidentiality NHS code of practice)

## Incident Management

Use risk Assessment data for input to:

* Business continuity plan,
* incident response (IR) plan,
* disaster recovery (DR) plan

[HSCC’s Operational Continuity Cyber incident](https://healthsectorcouncil.org/occi/) (OCCI) guidance and checklist

SAR - suspicious activity report

PIR - post incident review

## Audits

Internal Audits: Not independent reviewer

VS External Audits: independent reviewer

* Both Requires corrective action plan

Gap Analysis: gaps between identified risks and mitigating controls

Corrective Action Plan (CAP): enumerate resources required, identify milestones, schedule dates, assign responsibility, ensure access to resources

Mitigation Actions

* “Can it be tested?”
* Produced by a Trusted source
* Cost effective
* Addresses CIA
* Can be “backed out”
* Creates no additional security issues

NIST CSF: identify, protect, detect, respond, recover

POA&M - list of activities, resources required, responsible person, and date for completion

* Does not include system downtime or other factors

Destruction of information to reduce storage costs, keep relevant info, speed up indexing

# Third Party Risk Management

### Software

[HSCC’s supply chain risk management guide](https://healthsectorcouncil.org/HIC-SCRiM-v2/)

### Vendors

Vendors must comply with HITECH and HIPAA laws

* Have language in contract (BAA) w vendor/ business associate agreement
* [DHS will provide language](https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html) for HIPAA BAA
* [HSCC’s MC2](https://healthsectorcouncil.org/model-contract-language-for-medtech-cybersecurity-mc2/) contract

Primary organization should create Risk potential for the introducing 3rd party vendor that contains:

* Type of critical information shared w vendor
* nature of vendor’s service
* Amount and Type of data vendor has access to
* Frequency and sensitivity of data that is shared with vendor
* Method to access sensitive data
* ISO/SSAE compliance (certs requiring external review)
* Employee background checks for 3rd party under any contract where org has legal, reg, and risk management requirements for protected information
* Termination of 3rd parties has a high risk of leftover sensitive data. Destroy sensitive data as appropriate.

Developing Contract w 3rd party, ensure vendors

* Compliance
* Safeguards
* Right to audit
  + As You can’t ever fully transfer risk to vendor

Relationship Management

1. Set Expectations
2. Vendor Compliance
3. Ensure informed/privacy Safeguards
4. Audit vendor
5. Ensure Notification of breach
6. Location of access, storage, and processes
7. Vendor Data destruction
8. Vendor Employment verification
9. Vendor employee Training
10. Vendor subcontracting any work
11. Disaster recovery plan / business continuity

Triggers of 3rd party assessment

* The contract w vendor

ISA - interconnection service agreement. documents that outlines expectations between two organizations to address items such as technical specifications and configuration responsibilities for interconnection

Interconnection service agreement (ISA) contains:

* Security & privacy controls
* Network use
* Access limitations
* Confidentiality requirements
* Privileges
* Monitoring information