



HISPC 9-Domains



1. User and entity authentication to verify that a person or entity seeking access to electronic personal health information is who they claim to be.
 - The primary focus of this domain is to verify the user requesting access to Personal Health Information (PHI) is indeed who they claim to be and from the entity they claim to represent. This domain involves a review of the procedures applied assigning user IDs and passwords.



HISPC 9-Domains

2. Information authorization and access controls to allow access to only people or software programs that have been granted access rights to electronic personal health information.
 - How is access granted to the individual users? What controls are in place to ensure permissions are assigned appropriately and are not shared by multiple users? The primary focus is system security based on defined roles.



HISPC 9-Domains



3. Patient and provider identification to match identities across multiple information systems and locate electronic personal health information across enterprises.
 - This domain seeks consistency both within an entity and externally when requesting or sharing data. Discussion points to consider are public vs. private networks, research and other entities, and alternative access methods. Much of the discussion will focus on the master patient and provider indices.

HISPC 9-Domains

4. Information transmission security or exchange protocols (encryption, etc.) for information that is being exchanged over an electronic communications network.
 - In short how is the data altered or encrypted prior to transmission on a network. The goal is to prevent meaningful capture or access of data if intercepted by an unauthorized entity. Network examples include Wide Area Networks (WAN), Local Area Networks (LAN), or Virtual Private Networks (VPN).



HISPC 9-Domains



5. Information protections so that electronic personal health information cannot be improperly modified.
 - The primary question is how does an entity ensure modifications of the data are authorized to prevent abuse of access authority? This domain emphasizes the need for change management procedures or change control procedure logs relative to data access.



HISPC 9-Domains

6. Information audits that record and monitor the activity of health information systems.
 - HIPAA requires that audit trails of all data transactions be recorded for purposes of recovery and preserving data integrity. The audit trail will also identify any potential unauthorized access to PHI. Variables to consider include data backups and frequency, is the data modified for security purposes, and what data is tracked and how?



HISPC 9-Domains



7. Administrative or physical security safeguards required to implement a comprehensive security platform for Health Information Technology (HIT).
 - This domain is focused on the physical aspects of data security. It addresses the building housing the data, the room within the building, and access to the secured room itself. Discussion of this domain must include portable devices and the policies associated with ensuring security and controls away from the facility are administered.



HISPC 9-Domains



8. State law restrictions about information types and classes, and the solutions by which electronic personal health information can be viewed and exchanged.
 - Review of this domain involves legal variations in treatment of data. For example, behavior health opt in requirements vs. HIPAA opt out rules, general acute care procedures, pharmacy law, and how data release is authorized.



HISPC 9-Domains

9. Information use and disclosure policies that arise as health care entities share clinical health information electronically.
 - What are the consumers expectations of how data will be protected and administered? Is the patient notified of intent to use data and how their data will be shared with other entities such as research organizations and are there varying legal requirements depending on who the data is shared with?