

Minnesota Privacy and Security Project

Variations Working Group

Nine Domains of Privacy and Security

The Minnesota Privacy and Security Project will use the following nine, issue areas to examine scenarios related to the exchange of health information. Not all of the domain areas will apply to every scenario, but for each scenario we will try to determine which domains are relevant and how they interact with the scenario.

The complete list of the domains is provided on this front page for quick reference when considering the scenarios. A more detailed description that highlights the key dimensions of the domain and provides examples is provided in later pages.

Privacy and Security Reference List

- 1. User and entity authentication is used to verify that a person or entity seeking access to electronic personal health information is who they claim to be.**
- 2. Information authorization and access controls to allow access only to people or software programs that have been granted access rights to electronic personal health information.**
- 3. Patient and provider identification to match identities across multiple information systems and locate electronic personal health information across enterprises.**
- 4. Information transmission security or exchange protocols (i.e., encryption, etc.) for information that is being exchanged over an electronic communications network.**
- 5. Information protections so that electronic personal health information cannot be improperly modified.**
- 6. Information audits that record and monitor the activity of health information systems.**
- 7. Administrative or physical security safeguards required to implement a comprehensive security platform for health IT.**
- 8. State law restrictions about information types and classes, and the solutions by which electronic personal health information can be viewed and exchanged.**
- 9. Information use and disclosure policies that arise as health care entities share clinical health information electronically**

Privacy and Security Domain Descriptions and Examples

1. User and entity authentication is used to verify that a person or entity seeking access to electronic personal health information is who they claim to be.

Dimensions of business practice related to user or entity authentication:

- Use of digital signatures
- User authentication management
- Hardware/software authentication of software initiated requests for PHI
- Current business practices – user authentication
- Legal documentation related to user authentication
- Entity authentication

Examples of Business Practices:

Electronic environment:

- ✓ Policies and procedures requiring two passwords, hardware devices, such as a card key, or biometrics for user authentication.

Paper environment:

- ✓ Policies and procedures requiring employee photo identification badges or photo identification cards for user authentication.

2. Information authorization and access controls to allow access only to people or software programs that have been granted access rights to electronic personal health information.

Dimensions of business practices related to information authorization and access controls:

- Technology used to authenticate users/entities
- Technology used to control access to PHI
- Business practices implemented to control access to PHI
- User/entity validation methodology
- Legal documentation related to access control

Examples of Business Practices:

Electronic environment:

- ✓ Generally, security administration policies and procedures that control individual access permissions based upon their role or current responsibility.
- ✓ Security administration policies, procedures, and technology that allow for granular access control over protected health information.
- ✓ Security administration policies and procedures that require periodic review by data owners of access privileges to their systems.
- ✓ Access management controls that provide the ability to prevent specific user(s) from accessing designated health information.

Paper environment:

- ✓ Level of access to protected health information outlined in organizational job descriptions.
- ✓ Use of physical security devices such as key card access locks to security file rooms containing PHI.
- ✓ Organizational policies, procedures, and work processes designed to control access to protected health information.

3. Patient and provider identification to match identities across multiple information systems and locate electronic personal health information across enterprises.

Dimensions of business practices associated with patient and provider identification match:

- Types of patient identification used
- Types of provider identification used
- Common barriers related to different identification systems
- Implementation information related to implementing common identifier systems
- Consumer communication processes using common identifiers
- Methods used to validate provided identification

Examples of Business Practices:

Electronic environment:

- ✓ The record linking methods used to electronically link Master Patient Index records, electronic medical records, or external clinical results to existing electronic medical records can be applied at graduated levels.
- ✓ The use of work processes that employ basic record linking methods that compare selected data elements—most frequently name, birth date, Social Security number, or gender—using exact (identical match of data elements) and deterministic (exact or partial match) linking approaches.
- ✓ The use of work processes that employ intermediate record linking that include advanced techniques for comparing records by enhancing exact match and deterministic tools with additional logic and arbitrary or subjective scoring systems. Subjective weighting, ad-hoc weighting, fuzzy logic, and rules-based algorithms are examples of intermediate matching tools.
- ✓ The use of work processes that employ advanced record linking methods that employ sophisticated mathematical or statistical algorithms such as probabilistic matching, bipartite graph theory, machine learning, and neural networks.

Paper environment:

- ✓ The vast majority of health care providers with paper-based or hybrid electronic medical record systems currently use electronic master patient indexing systems. The record linking methods described above would be employed.

4. Information transmission security or exchange protocols (i.e., encryption, etc.) for information that is being exchanged over an electronic communications network.

Dimensions of business practices associated with transmission security and exchange protocols:

- Types of transmission protection implemented (i.e., VPN, secure FTP, encrypted e-mail, secure web communication, application layer secure communication, etc.)
- Vendors used to implement secure transmission of data
- Business processes established to ensure secure transmission
- Inter-organizational processes/practices implemented to seamlessly communicate securely between entities
- Secure data transmission processes established between the entity and the consumer

Examples of Business Practices:

Electronic environment:

- ✓ Transmission security policies and procedures that mandate that security transmission requirements have been discussed and compliance agreed upon by identified key personnel involved in the transmission of electronic PHI before any health information is exchanged between disparate entities.
- ✓ All EHR System users are aware of and have received training in transmission security policies and procedures.

Paper environment:

- ✓ When faxing PHI, all faxes contain a statement at the bottom indicating that the fax is intended only for the party listed above and that if it is received by the wrong party, they should call the sending party immediately. Often the sending party will call the receiving party to verify receipt.

5. Information protections so that electronic personal health information cannot be improperly modified.

Dimensions of business practices associated with protection against improper modification of personal health information:

- Established data integrity processes, policies and procedures (within & between entities)

- Legal documentation developed to address data integrity
- Vendors used to provide software that allows protection from data modification
- Barriers to implementing data integrity processes between organizations (i.e., protecting data from improper alteration while allowing modification for appropriate purposes such as treatment)
- Data integrity validation processes (within & between entities; business processes & technology)
- Notification processes documenting when data needs to be modified for appropriate purposes such as treatment

Examples of Business Practices:

Electronic environment:

- ✓ An auditing process is employed using trained professionals to monitor and verify that electronic PHI has been protected from unauthorized access during transmission in compliance with approved policy and procedure.
- ✓ Security administrative controls that mandate separation of duties for key system change privileges.
- ✓ System administrative controls that shall retain all data modified until otherwise purged, deleted, archived, or otherwise deliberately removed from the system by security administrators.
- ✓ The system shall provide the functionality to allow the patient to review and contest health information documented in their medical record.

Paper environment:

- ✓ Anytime a record is reported to contain documentation regarding an adverse event or some other incident, it is placed in a special locked file. A copy is made for clinical use. Anyone wishing to review the original record can do so with the Release of Information Supervisor by their side ensuring the documentation is not altered.

6. Information audits that record and monitor the activity of health information systems.

Dimensions of business practices associated with recording and monitoring of systems:

- Types of audit logs currently used by entities to monitor healthcare data activity, transmission, etc.
- Examples of audit programs established to evaluate appropriate privacy & security practices are being followed
- Inter-organization data access audit logs established
- Use of external audit resources and what those resources are
- Audit log data sharing agreements (if available)
- Barriers to creation of and analysis of audit logs (i.e., installed use of legacy software, lack of software audit log creation capability, etc.)

Examples of Business Practices:

Electronic and/or paper environment:

- ✓ An auditing process is employed utilizing trained professionals to monitor and verify that electronic PHI has been protected from unauthorized access or tampering in compliance with approved security administration policy and procedure.
- ✓ Each time a file containing PHI is printed or copied the EHR system shall record the date, time, and system user for each occurrence to the audit activity file.
- ✓ Record movement within the organization is tracked via a manual or computer-based log application.
- ✓ A bar-coded record locator system is used to track the movements of all patient records.

7. Administrative or physical security safeguards required to implement a comprehensive security platform for health IT

Dimensions of business practices associated with administrative and physical safeguards:

- Established business practices to reasonably ensure administrative security
- Established business practices to reasonably ensure physical security
- Examples of legal documentation developed between entities outlining appropriate administrative & physical security practices
- Inter-organization established business processes addressing administrative & physical security
- Legal documentation drafted to reasonably ensure administrative & physical security between entities
- Administrative & physical security practices at it relates to customer interaction
- Implementation plans developed that address compliance with the HIPAA Security Rule & applicable state law.

Examples of Business Practices:

Electronic environment:

- All EHR System users are aware of and have received training on system security administration policies and procedures.
- Security administration policies and procedures based upon the principles of “least privilege” and “separation of duties”.
- Security administration policies and procedures that control individual access permissions based upon their role or current responsibility.
- Security administration polices, procedures, and technology that allow for granular access control “separation of duties” over protected health information.

- Security administration policies and procedures that require periodic review by data owners of access privileges to their systems.
- The system shall provide the functionality to allow the patient to review and contest health information documented in their medical record.

Paper environment:

- Storage areas for patient records are located above the basement to protect against floods. Further, gas fire extinguishing systems are installed to protect against water damage in the event of a fire.
- Persons are not allowed access to areas with PHI without an appropriate ID.

8. State law restrictions about information types and classes, and the solutions by which electronic personal health information can be viewed and exchanged.

Dimensions of Business Practice:

- State laws that preempt HIPAA
- Barriers that hamper data sharing between individuals or entities because of established state laws
- Solutions adopted to address data sharing between individuals or entities where state law is more stringent than HIPAA
- Inter-state data exchange barriers & solutions
- Recommended changes at the state & federal level to address conflicting laws
- Legal documentation developed to address more stringent state law (intra and inter-state)

Examples of Business Practices

Electronic and/or paper environment:

- ✓ Psychiatric health information exchange may only be conveyed via direct physician-to-physician contact.
- ✓ Any release of psychiatric health information can only be initialed by a specific authorization signed by the patient or legal guardian of the patient.
- ✓ Any non-emergent health information exchange that includes document of HIV requires a special authorization signed by the patient before the information can be exchanged.

9. Information use and disclosure policies that arise as health care entities share clinical health information electronically.

Dimensions of business practices associated with use and disclosure policies:

- Implemented information use & disclosure policies
- Barriers to implementation of information use & disclosure policies between entities & individuals

- Solutions that address adoption of workable information use & disclosure policies between entities & individuals
- Legal documentation created to address appropriate & workable adoption of information use & disclosure policies
- Business practices related to information use & disclosure between entities
- Business practices related to information use & disclosure between entities & consumers
- Technology implemented to track appropriate information use & disclosure
- Methods used to track appropriate information use & disclosure

Examples of Business Practices

Electronic and/or paper environment:

- ✓ Entity business policies limit electronic health information exchange to facsimile transmission.
- ✓ Entity business policies and procedures that require all requested health information to be printed out for health information exchange.
- ✓ Entity business policies and procedures that prevent the exchange of all dictated and transcribed health information documents until they have been reviewed and signed by the author.
- ✓ Entity business policy requiring any subcontractor handling information be chartered in the United States so they are subject to HIPAA.