Tool 2. Dimensions of Business Practices

Tool 2. Dimensions of Business Practices[1]

This document describes the dimensions of business practices associated with each of the 9 domains of privacy and security defined for the project and provides illustrative examples of business practices reported during the pilot study.

Privacy and Security Domain 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.

Dimensions of Business Practice:

- Use of digital signatures or digital certificates
- User authentication management and audit
- Hardware/software authentication of software-initiated requests by individuals or entities for personal health information
- Role-based access management and associated authentication
- Current business practices—user authentication
- Legal documentation related to user authentication
- Entity authentication

Examples of Business Practices:

Electronic environment:

- Policies and procedures require unique user IDs, passwords, hardware devices such as card keys or security tokens, or biometrics for user authentication.

Paper environment:

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

[1] Chris Apgar, CISSP, Apgar and Associates, LLC.

Privacy and Security Domain 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 Practice:

- Technology used to authenticate users/entities
- Technology used to control access to personal health information
- Business practices implemented to control access to personal health information
- User/entity validation methodology
- Audit controls to monitor access and appropriate use of authorization
- Legal documentation related to access control

Examples of Business Practices:

Electronic environment:

- Security administration policies and procedures control access permissions according to individuals' roles and responsibilities.
- Security administration policies, procedures, and technology allow granular access control over personal health information.
- Security administration policies and procedures require periodic review by data owners of access privileges to their systems.
- Access management controls provide the ability to prevent specific user(s) from accessing designated health information.
- Audit log generation capabilities are included with regular granular and general audits.
- Appropriate sanctions are applied for misuse of access privileges.

Paper environment:

- Level of access to personal health information is outlined in organizational job descriptions.
- Physical security devices are used, such as key card access locks to security file rooms containing personal health information.
- Organizational policies, procedures, and work processes are designed to control access to personal health information.
- A check-in/check-out log is used to record use and return of medical records.
- An associated audit of the check-in/check-out log is conducted, along with spot checks of file use by workforce members.

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

Dimensions of Business Practice:

- 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 provider and patient 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.
- Basic record linking methods 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.
- Intermediate record linking methods 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.
- Advanced record linking methods are based on sophisticated mathematical or statistical algorithms such as probabilistic matching, bipartite graph theory, machine learning, and neural networks.
- Appropriate authentication mechanisms are used to validate provider and/or patient identity.

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 are employed.

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

Dimensions of Business Practice:

- Types of transmission protection implemented (virtual private network [VPN], secure file transfer protocol [FTP], encrypted e-mail, secure web communication, application layer secure communication, etc)
- Vendors or vendor-supplied applications and appliances used to implement secure transmission of data
- Business processes established to ensure secure transmission of personal health information
- Interorganizational processes/practices implemented to seamlessly communicate securely between entities
- Secure data transmission processes established between the entity and any remote members of the entity's workforce
- Secure data transmission processes established between the entity and the consumer

Examples of Business Practices:

Electronic environment:

- Security policies and procedures mandate that security transmission requirements be discussed and compliance agreed upon by identified key personnel at disparate entities before they exchange any electronic personal health information.
- All electronic health record (EHR) system users are aware of and have received training in transmission security policies and procedures.
- Appropriate technical solutions have been acquired and implemented, and staff have been trained to use them.
- Transmission of data on media or portable devices is secured before leaving a secure environment.
- Appropriate audit practices have been adopted.
- Appropriate sanctions are applied for transmission of unencrypted personal health information.

Paper environment:

- All faxes of personal health information contain a statement at the bottom indicating that the fax is intended only for the party listed and that if it is received by the wrong party, he or she should call the sending party immediately. Often the sending party will call the receiving party to verify receipt.
- Appropriate practices have been adopted to secure fax transmission.
- Secure methods have been established for transporting paper files.

Privacy and Security Domain 5
Information protections so that electronic personal health information cannot be improperly modified.

Dimensions of Business Practice:

- Established data integrity processes, policies, and procedures (within and between entities or individuals)
- Legal documentation related to data integrity
- Vendors or vendor-supplied application or appliance used to provide software that allows protection from data modification or destruction
- Barriers to implementing data integrity processes between organizations (ie, protecting data from improper alteration while allowing modification for appropriate purposes such as treatment)
- Data integrity validation processes (within and between entities or individuals, including business processes and technology)
- Notification processes documenting when data needs to be modified for appropriate purposes such as treatment
- Use of encryption when sending data between entities and/or individuals
- Adoption of appropriate data backup and recovery policies, procedures, and practices to ensure recovery of lost or corrupted data
- Use of digital signatures to provide nonrepudiation protection

Examples of Business Practices:

Electronic environment:

- An auditing process is employed using trained professionals to monitor and verify that electronic personal health information has been protected from unauthorized access during transmission, in compliance with approved policies and procedures.
- Security administrative controls mandate separation of duties for key system change privileges.
- System administrative controls are in place that retain all data modified until purged, deleted, archived, or otherwise deliberately removed from the system by security administrators.
- Patients are able to review and contest health information documented in their medical record.
- Data backups are securely transported and stored off site, and recovery of data from backups is tested regularly.

Paper environment:

- Records reported to contain documentation on an adverse event or other incident are secured in a locked file. A copy is made for clinical use. Original records can only be reviewed if accompanied by the Release of Information Supervisor, preventing the alteration of the record.

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

Dimensions of Business Practice:

- Types of audit logs currently used by entities to monitor health care data activity, transmission, etc.
- Examples of audit programs established to evaluate appropriate privacy and security practices
- Interorganization data access audit logs established and periodically reviewed
- Use of external audit resources and descriptions of external audit resources
- Audit log data sharing agreements (if available)
- Barriers to creation of and analysis of audit logs (installed use of legacy software, lack of software audit log creation capability, etc)
- Appropriate retention of audit documentation
- Implementation and enforcement of appropriate sanction policies covering entities and individuals

Examples of Business Practices:

Electronic and/or paper environment:

- An auditing process is employed using trained professionals (internal or external) to monitor and verify that electronic personal health information has been protected from unauthorized access or tampering, in compliance with approved security administration policies and procedures.
- Audit staff have the authority to take action as necessary.
- Each time a file containing personal health information is printed or copied, the EHR system records the date, time, and system user to the audit activity file.
- Audit logs are created and reviewed to record any instance of an entity or individual accessing, modifying, creating, destroying, deleting, or transmitting personal health information.
- Movement of records or personal health information 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.

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

Dimensions of Business Practice:

- Established business practices to reasonably ensure administrative security
- Established business practices to reasonably ensure physical security
- Examples of legal documentation developed between entities or individuals outlining appropriate administrative and physical security practices
- Interorganization established business processes addressing administrative and physical security
- Legal documentation drafted to reasonably ensure administrative and physical security between entities
- Administrative and physical security practices as they relate to customer interaction
- Adoption of common policies and procedures between organizations for the privacy and security of personal health information
- Implementation plans developed that address compliance with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule and applicable state law
- Adoption of an audit program to reasonably ensure that participating entities and individuals are following established policies, procedures, and practices

Examples of Business Practices:

Electronic environment:

- All EHR system users are aware of and have received training on security policies and procedures (including any requirements more stringent than HIPAA).
- Security administration policies and procedures are based on principles of *least privilege* and *separation of duties*.
- Security administration policies and procedures control individual, entity, and automated access permissions according to roles, requirements, or current responsibilities.
- Security administration policies, procedures, and technology allow granular access control over personal health information by applying "separation of duties" principles.
- Security administration policies and procedures require periodic review by data owners of access privileges to their systems and commonly maintained data.
- System functionality allows patients to review and request amendments to health information documented in their medical or claims 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 containing personal health information without an appropriate ID.
- Appropriate privacy and security policies, procedures, and practices are in place to reasonably ensure confidentiality of personal health information.
- Policies, procedures, and practices have been established to allow patient access to health records and provide the opportunity to request amendment.

Privacy and Security Domain 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 are more stringent than HIPAA and 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
- Interstate data exchange barriers and solutions
- Recommended changes at the state and federal levels to address conflicting laws
- Legal documentation developed to address more stringent state law (intra- and interstate)
- Adoption of standard industry practices related to sharing specially protected data

Examples of Business Practices

Electronic and/or paper environment:

- Psychiatric health information exchange may only be conveyed via direct physician-to-physician contact, with appropriate authorization.
- Any nonemergent health information exchange that includes documentation of HIV requires a special authorization signed by the patient before the information can be exchanged.
- Authorization policies, procedures, and templates have been adopted, and workforce members are trained on special restrictions.

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

Dimensions of Business Practice:

- Implemented standardized information use and disclosure policies
- Barriers to implementation of information use and disclosure policies between entities and individuals
- Solutions that address adoption of workable information use and disclosure policies, procedures, and practices between entities and individuals
- Legal documentation created to address appropriate and workable adoption of information use and disclosure policies
- Business practices related to information use and disclosure between entities
- Business practices related to information use and disclosure between entities and consumers
- Technology implemented to track appropriate information use and disclosure
- Implementation of appropriate audit practices
- Methods used to track appropriate information use and 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 require that all requested health information be printed out for health information exchange.
- Entity business policies and procedures prevent the exchange of all dictated and transcribed health information documents until they have been reviewed and signed by the author.
- Entity business policies and procedures require that any subcontractor handling information sign and adhere to a business associate agreement.
- Standard business associate contracts are used with third parties who have access to personal health information and who perform services on behalf of the entity or individual.
- Policies, procedures, and practices prohibit health information exchange with another entity or individual unless the information is properly encrypted.