TECHNICAL SECURITY SERVICES TO GUARD DATA INTEGRITY, CONFIDENTIALITY, AND AVAILABILITY—Continued

Requirement	Implementation
Entity Authentication (The following implementation features must be implemented: Automatic logoff, Unique user identification. In addition, at least one of the other listed implementation features must be implemented).	Automatic logoff. Biometric. Password. PIN. Telephone callback. Token. Unique user identification.

TECHNICAL SECURITY MECHANISMS TO GUARD AGAINST UNAUTHORIZED ACCESS TO DATA THAT IS TRANSMITTED OVER A COMMUNICATIONS NETWORK

Requirement	Implementation
Communications/network controls (The following implementation features must be implemented: Integrity controls, Message authentication. If communications or networking is employed, one of the following implementation features must be implemented: Access controls, Encryption. In addition, if using a network, the following four implementation features must be implemented: Alarm, Audit trail, Entity authentication, Event reporting).	Access controls. Alarm. Audit trail. Encryption. Entity authentication. Event reporting. Integrity controls. Message authentication.

ELECTRONIC SIGNATURE

Requirement	Implementation
Digital signature (If digital signature is employed, the following three implementation features must be implemented: Message integrity, Non-repudiation, User authentication. Other implementation features are optional).	Ability to add attributes. Continuity of signature capability. Counter signatures. Independent verifiability. Interoperability. Message integrity. Multiple Signatures. Non-repudiation. Transportability. User authentication.

Addendum 2—HIPAA Security and Electronic Signature Standards Glossary of Terms

Please Note:

(1) While we have attempted to categorize security requirements for ease of understanding and reading clarity, there are overlapping areas on the matrix in which the same requirements are restated in a slightly different context.

(2) While not appearing on the matrix, a number of terms listed below do appear in the glossary descriptions and have been supplied for additional clarity:

(3) The definitions provided in this document have been obtained from multiple sources.

Ability to add attributes:
- One possible capability of a digital signature technology, for example, the ability to add a time stamp as part of a digital signature.
- Part of digital signature on the matrix.

Access:
- The ability or the means necessary to read, write, modify, or communicate data/information or otherwise make use of any system resource.

Access authorization:
- Information-use policies/procedures that establish the rules for granting and/or restricting access to a user, terminal, transaction, program, or process.
- Part of information access control on the matrix.

Access control:
- A method of restricting access to resources, allowing only privileged entities access. (PGP, Inc.)
- Types of access control include, among others, mandatory access control, discretionary access control, time-of-day, classification, and subject-object separation.
- Part of Media Controls on the matrix.
- Part of technical security services to control and monitor access to information on the matrix.

Access controls:
- The protection of sensitive communications transmissions over open or private networks so that it cannot be easily intercepted and interpreted by parties other than the intended recipient.
- Part of mechanisms to prevent unauthorized access to data that is transmitted over a communications network on the matrix.

Access establishment:
- The security policies, and the rules established therein, that determine an entity's initial right of access to a terminal, transaction, program, or process.
- Part of information access control on the matrix.

Access Level:
- A level associated with an individual who may be accessing information (for example, a clearance level) or with the information which may be accessed (for example, a classification level). (NRC, 1991, as cited in HISB, DRAFT GLOSSARY OF TERMS RELATED TO INFORMATION SECURITY IN HEALTH CARE INFORMATION SYSTEMS draft Glossary of Terms Related to Information Security in Health Care Information Systems)

Access modification:
- The security policies, and the rules established therein, that determine types of, and reasons for, modification to an entity's established right of access to a terminal, transaction, program, or process.
- Part of information access control on the matrix.

Accountability:
- The property that ensures that the actions of an entity can be traced uniquely to that entity. (ASTM E1762—95)

Part of media controls on the matrix.

Administrative procedures to guard data integrity, confidentiality and availability:
Documented, formal practices to manage (1) the selection and execution of security measures to protect data, and (2) the conduct of personnel in relation to the protection of data.
A section of the matrix.

Alarm, event reporting, and audit trail:
(1) Alarm: In communication systems, any device that can sense an abnormal condition within the system and provide, either locally or remotely, a signal indicating the presence of the abnormality. (188) NOTE: The signal may be in any desired form ranging from a simple contact closure (or opening) to a time-phased automatic shutdown and restart cycle. (Glossary of INFOSEC and INFOSEC Related Terms—Idaho State University)
(2) Event reporting: Network message indicating operational irregularities in physical elements of a network or a response to the occurrence of a significant task, typically the completion of a request for information. (Glossary of INFOSEC and INFOSEC Related Terms—Idaho State University)
(3) Audit trail: Data collected and potentially used to facilitate a security audit. (ISO 7498–2, as cited in HISB, DRAFT GLOSSARY OF TERMS RELATED TO INFORMATION SECURITY IN HEALTH CARE INFORMATION SYSTEMS draft Glossary of Terms Related to Information Security in Health Care Information Systems)
Part of mechanisms to prevent unauthorized access to data that is transmitted over a communications network on the matrix.

Applications and data criticality analysis:
An entity's formal assessment of the sensitivity, vulnerabilities, and security of its programs and information it receives, manipulates, stores, and/or transmits.
Part of contingency plan on the matrix.

Assigned security responsibility:
Practices put in place by management to manage and supervise (1) the execution and use of security measures to protect data, and (2) the conduct of personnel in relation to the protection of data.
Part of Physical safeguards to guard data integrity, confidentiality, and availability on the matrix.

Assure supervision of maintenance personnel by authorized, knowledgeable person:
Documented formal procedures/instruction for the oversight of maintenance personnel when such personnel are in the vicinity of health information pertaining to an individual.
Part of personnel security on the matrix.

Asymmetric encryption:
Encryption and decryption performed using two different keys, one of which is referred to as the public key and one of which is referred to as the private key.
Also known as public-key encryption. (Stallings)

Asymmetric key:
One half of a key pair used in an asymmetric (''public-key'') encryption system. Asymmetric encryption systems have two important properties: (1) the key used for encryption is different from the one used for decryption (2) neither key can feasibly be derived from the other. (CORBA Security Services, 1997)

Audit controls:
The mechanisms employed to record and examine system activity.
Part of technical security services to control and monitor access to information on the matrix.

Authorization control:
The mechanism for obtaining consent for the use and disclosure of health information.
Part of technical security services to control and monitor access to information on the matrix.

Automatic logoff:
After a pre-determined time of inactivity (for example, 15 minutes), an electronic session is terminated.
Part of entity authentication on the matrix.

Availability:
The property of being accessible and useable upon demand by an authorized entity. (ISO 7498–2, as cited in the HISB draft Glossary of Terms Related to Information Security In Health care Information Systems)

Awareness training for all personnel (including management):
All personnel in an organization should undergo security awareness training, including, but not limited to, password maintenance, incident reporting, and an education concerning viruses and other forms of malicious software.
Part of Training on the matrix.

Biometric:.
A biometric identification system identifies a human from a measurement of a physical feature or repeatable action of the individual (for example, hand geometry, retinal scan, iris scan, fingerprint patterns, facial characteristics, DNA sequence characteristics, voice prints, and hand written signature). (ASTM E1762—95, as cited in the HISB draft Glossary of Terms Related to Information Security In Health care Information Systems)
Part of entity authentication on the matrix.

Certification:
The technical evaluation performed as part of, and in support of, the accreditation process that establishes the extent to which a particular computer system or network design and implementation meet a pre-specified set of security requirements. This evaluation may be performed internally or by an external accrediting agency.
Part of administrative procedures to guard data integrity, confidentiality, and availability.

Chain of Trust Partner Agreement:
Contract entered into by two business partners in which it is agreed to exchange data and that the first party will transmit information to the second party, where the data transmitted is agreed to be protected between the partners. The sender and receiver depend upon each other to maintain the integrity and confidentiality of the transmitted information. Multiple such two-party contracts may be involved in moving information from the originator to the ultimate recipient, for example, a provider may contract with a clearing house to transmit claims to the clearing house; the clearing house, in turn, may contract with another clearing house or with a payer for the further transmittal of those same claims.
Part of administrative procedures to guard data integrity, confidentiality and availability on the matrix..

Classification:
Protection of data from unauthorized access by the designation of multiple levels of access authorization clearances to be required for access, dependent upon the sensitivity of the information.
A type of access control on the matrix.

Clearing House:
* * * a public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements. (HIPAA, Subtitle F, Section 262(a) Section 1171(2))

Combination locks changed:
Documented procedure for changing combinations of locking mechanisms, both on a recurring basis and when personnel knowledgeable of combinations no longer have a need to know or a requirement for access to the protected facility/system.
Part of termination procedures on the matrix.

Confidentiality:
The property that information is not made available or disclosed to unauthorized individuals, entities or processes. (ISO 7498–2, as cited in the HISB draft Glossary of Terms Related to Information Security In Health care Information Systems) .

Context-based access:
An access control based on the context of a transaction (as opposed to being based on attributes of the initiator or target). The ''external'' factors might include time of day, location of the user, strength of user authentication, etc.
Part of access control on the matrix.

Contingency Plan:
A plan for responding to a system emergency. The plan includes performing backups, preparing critical facilities that can be used to facilitate continuity of operations in the event of an emergency, and recovering from a disaster. (O'Reilly, 1992, as cited in the HISB draft Glossary of Terms Related to Information Security In Health care Information Systems) Contingency plans should be updated routinely.
Part of Administrative procedures to guard data integrity, confidentiality and availability on the matrix.

Continuity of signature capability:
The public verification of a signature shall not compromise the ability of the signer to apply additional secure signatures at a later date. (ASTM E 1762—95)

Part of digital signature on the matrix.

Counter signatures:
It shall be possible to prove the order of application of signatures. This is analogous to the normal business practice of countersignatures, where some party signs a document which has already been signed by another party. (ASTM E 1762 -95)
Part of digital signature on the matrix.

Data:
A sequence of symbols to which meaning may be assigned. (NRC, 1991, as cited in the HISB draft Glossary of Terms Related to Information Security In Health care Information Systems)

Data authentication:
The corroboration that data has not been altered or destroyed in an unauthorized manner. Examples of how data corroboration may be assured include the use of a check sum, double keying, a message authentication code, or digital signature.
Part of technical security services to control and monitor access to information on the matrix

Data backup:
A retrievable, exact copy of information.
Part of media controls on the matrix.

Data backup plan:
A documented and routinely updated plan to create and maintain, for a specific period of time, retrievable exact copies of information.
Part of contingency plans on the matrix.

Data Integrity:
The property that dat has [sic] not been altered or destroyed in an unauthorized manner. (ASTM E1762–95).

Data storage:
The retention of health care information pertaining to an individual in an electronic format.
Part of media controls on the matrix.

Digital signature:
An electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified. (FDA Electronic Record; Electronic Signatures; Final Rule)
Part of electronic signature on the matrix.

Disaster recovery:
The process whereby an enterprise would restore any loss of data in the event of fire, vandalism, natural disaster, or system failure. (CPRI, 1996c, as cited in HISB, DRAFT GLOSSARY OF TERMS RELATED TO INFORMATION SECURITY IN HEALTH CARE INFORMATION SYSTEMS draft Glossary of Terms Related to Information Security in Health Care Information Systems)
Part of physical access controls (limited access) on the matrix.

Disaster recovery plan:
Part of an overall contingency plan. The plan for a process whereby an enterprise would restore any loss of data in the event of fire, vandalism, natural disaster, or system failure. (CPRI, 1996c, as cited in HISB, DRAFT GLOSSARY OF TERMS RELATED TO INFORMATION SECURITY IN HEALTH CARE INFORMATION SYSTEMS draft Glossary of Terms Related to Information Security in Health Care Information Systems)
Part of contingency plan on the matrix.

Discretionary access control:
Discretionary Access Control (DAC) is used to control access by restricting a subject's access to an object. It is generally used to limit a user's access to a file. In this type of access control it is the owner of the file who controls other users' accesses to the file.
A type of access control on the matrix.

Disposal:
The final disposition of electronic data, and/or the hardware on which electronic data is stored.
Part of media controls on the matrix.

Documentation:
Written security plans, rules, procedures, and instructions concerning all components of an entity's security.
Part of security configuration mgmt on the matrix.

Electronic data interchange (EDI):
Intercompany, computer-to-computer transmission of business information in a standard format. For EDI purists, ''computer-to-computer'' means direct transmission from the originating application program to the receiving, or processing, application program, and an EDI transmission consists only of business data, not any accompanying verbiage or free-form messages. Purists might also contend that a standard format is one that is approved by a national or international standards organization, as opposed to formats developed by industry groups or companies. (EDI Security, Control, and Audit)

Electronic signature:
The attribute that is affixed to an electronic document to bind it to a particular entity. An electronic signature process secures the user authentication (proof of claimed identity, such as by biometrics (fingerprints, retinal scans, hand written signature verification, etc.), tokens or passwords) at the time the signature is generated; creates the logical manifestation of signature (including the possibility for multiple parties to sign a document and have the order of application recognized and proven) and supplies additional information such as time stamp and signature purpose specific to that user; and ensures the integrity of the signed document to enable transportability, interoperability, independent verifiability, and continuity of signature capability. Verifying a signature on a document verifies the integrity of the document and associated attributes and verifies the identity of the signer. There are several technologies available for user authentication, including passwords, cryptography, and biometrics. (ASTM 1762–95, as cited in the HISB draft Glossary of Terms Related to Information Security In Health care Information Systems)

Emergency mode operation:
Access controls in place that enable an enterprise to continue to operate in the event of fire, vandalism, natural disaster, or system failure.
Part of physical access controls (limited access) on the matrix.

Emergency mode operation plan:
Part of an overall contingency plan. The plan for a process whereby an enterprise would be able to continue to operate in the event of fire, vandalism, natural disaster, or system failure.
Part of contingency plan on the matrix.

Encryption:
Transforming confidential plaintext into ciphertext to protect it. Also called encipherment. An encryption algorithm combines plaintext with other values called keys, or ciphers, so the data becomes unintelligible. Once encrypted, data can be stored or transmitted over unsecured lines. (EDI Security, Control, and Audit)
Decrypting data reverses the encryption algorithm process and makes the plaintext available for further processing.
Part of access control on the matrix.

Entity authentication:
1. The corroboration that an entity is the one claimed. (ISO 7498–2, as cited in the HISB draft Glossary of Terms Related to Information Security In Health care Information Systems)
Part of technical security services to control and monitor access to information on the matrix.
2. A communications/network mechanism to irrefutably identify authorized users, programs, and processes, and to deny access to unauthorized users, programs and processes.
Part of mechanisms to prevent unauthorized access to data that is transmitted over a communications network on the matrix.

Equipment control (into and out of site):
Documented security procedures for bringing hardware and software into and out of a facility and for maintaining a record of that equipment. This includes, but is not limited to, the marking, handling, and disposal of hardware and storage media.
Part of physical access controls (limited access) on the matrix.

Facility security plan:
A plan to safeguard the premises and building(s) (exterior and interior) from unauthorized physical access, and to safeguard the equipment therein from unauthorized physical access, tampering, and theft.
Part of physical access controls (limited access) on the matrix.

Formal mechanism for processing records:
Documented policies and procedures for the routine, and non-routine, receipt, manipulation, storage, dissemination, transmission, and/or disposal of health information.

Part of administrative procedures to guard data integrity, confidentiality, and availability on the matrix.

Hardware/software installation & maintenance review and testing for security features:
Formal, documented procedures for (1) connecting and loading new equipment and programs, (2) periodic review of the maintenance occurring on that equipment and programs, and (3) periodic security testing of the security attributes of that hardware/software.
Part of security configuration mgmt on the matrix.

Independent verifiability:
The capability to verify the signature without the cooperation of the signer. Technically, it is accomplished using the public key of the signatory, and it is a property of all digital signatures performed with asymmetric key encryption
Part of digital signature on the matrix.

Information:
Data to which meaning is assigned, according to context and assumed conventions. (National Security Council, 1991, as cited in the HISB draft Glossary of Terms Related to Information Security In Health care Information Systems)

Information access control:
Formal, documented policies and procedures for granting different levels of access to health care information.
Part of administrative procedures to ensure integrity and confidentiality on the matrix.

Integrity controls:
Security mechanism employed to ensure the validity of the information being electronically transmitted or stored.
Part of mechanisms to prevent unauthorized access to data that is transmitted over a communications network on the matrix.

Internal audit:
The in-house review of the records of system activity (for example, logins, file accesses, security incidents) maintained by an organization.
Part of administrative procedures to guard data integrity, confidentiality, and availability on the matrix.

Interoperability:
The applications used on either side of a communication, between trading partners and/or between internal components of an entity, being able to read and correctly interpret the information communicated from one to the other.
Part of digital signature on the matrix.

Inventory:
Formal, documented identification of hardware and software assets.
Part of security configuration mgmt on the matrix.

Key:
An input that controls the transformation of data by an encryption algorithm (NRC, 1991, as cited in the HISB draft Glossary of Terms Related to Information Security In Health care Information Systems)

Maintenance of record of access authorizations:
Ongoing documentation and review of the levels of access granted to a user, program, or procedure accessing health information.
Part of personnel security on the matrix.

Maintenance records:
Documentation of repairs and modifications to the physical components of a facility, for example, hardware, software, walls, doors, locks.
Part of physical access controls (limited access) on the matrix.

Mandatory Access Control (MAC):
A means of restricting access to objects that is based on fixed security attributes assigned to users and to files and other objects. The controls are mandatory in the sense that they cannot be modified by users or their programs. (Stallings, 1995) (as cited in the HISB draft Glossary of Terms Related to Information Security In Health care Information Systems)
A type of access control on the matrix.

Media controls:
Formal, documented policies and procedures that govern the receipt and removal of hardware/software (for example, diskettes, tapes) into and out of a facility.
Part of physical safeguards to guard data integrity, confidentiality, and availability on the matrix.

Message:
A digital representation of information. (ABA Digital Signatures Guidelines)

Message authentication:
Ensuring, typically with a message authentication code, that a message received (usually via a network) matches the message sent. (O'Reilly, 1992, as cited in the HISB draft Glossary of Terms Related to Information Security In Health care Information Systems)
Part of mechanisms to prevent unauthorized access to data that is transmitted over a communications network on the matrix

Message authentication code:
Data associated with an authenticated message that allows a receiver to verify the integrity of the message. (Glossary of INFOSEC and INFOSEC Related Terms—Idaho State University)

Message integrity:
The assurance of unaltered transmission and receipt of a message from the sender to the intended recipient. (ABA Digital Signature Guidelines)
Part of digital signature on the matrix.

Multiple signatures:
It shall be possible for multiple parties to sign a document. Multiple signatures are conceptually, simply appended to the document. (ASTM E 1762–95)
Part of digital signature on the matrix.

Need-to-know procedures for personnel access:
A security principle stating that a user should have access only to the data he or she needs to perform a particular function. (O'Reilly, 1992, as cited in the HISB draft Glossary of Terms Related to Information Security In Health care Information Systems)
Part of physical access controls (limited access) on the matrix.

Nonrepudiation:
Strong and substantial evidence of the identity of the signer of a *message* and of message integrity, sufficient to prevent a party from successfully denying the origin, submission or delivery of the message and the integrity of its contents. (ABA Digital Signature Guidelines)
Part of digital signature on the matrix.

Operating, and in some cases, maintenance personnel have proper access authorizations:
Formal, documented policies and procedures to be followed in determining the access level to be granted to individuals working on, or in the vicinity of, health information.
Part of personnel security on the matrix.

Password:
Confidential authentication information composed of a string of characters. (ISO 7498—2, as cited in the HISB draft Glossary of Terms Related to Information Security In Health care Information Systems)
Part of entity authentication on the matrix.

Periodic security reminders:
Employees, agents and contractors should be made aware of security concerns on an ongoing basis.
Part of training on the matrix.

Personnel clearance procedure:
A protective measure applied to determine that an individual's access to sensitive unclassified automated information is admissible. The need for and extent of a screening process is normally based on an assessment of risk, cost, benefit, and feasibility as well as other protective measures in place. Effective screening processes are applied in such a way as to allow a range of implementation, from minimal procedures to more stringent procedures commensurate with the sensitivity of the data to be accessed and the magnitude of harm or loss that could be caused by the individual (DOE 1360.2A, as cited in Glossary of INFOSEC and INFOSEC Related Terms—Idaho State University)
Part of personnel security on the matrix.

Personnel security:
The procedures established to ensure that all personnel who have access to sensitive information have the required authority as well as appropriate clearances. (NCSC Glossary of Computer Security Terms, October 21, 1988)
Part of administrative procedures to guard data integrity, confidentiality and availability on the matrix.

Personnel security policy/procedure:
Formal, documentation of policies and procedures established to ensure that all personnel who have access to sensitive information have the required authority as well as appropriate clearances. (Glossary of INFOSEC and INFOSEC Related Terms—Idaho State University)
Part of personnel security on the matrix.

Physical access controls (limited access):
Those formal, documented policies and procedures to be followed to limit

physical access to an entity while ensuring that properly authorized access is allowed.
Part of Physical safeguards to guard data integrity, confidentiality, and availability on the matrix.

Physical safeguards:
Protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion. Also covers the use of locks, keys, and administrative measures used to control access to computer systems and facilities. (O'Reilly, 1992, as cited in HISB, draft Glossary of Terms Related to Information Security in Health Care Information Systems)
A section of the matrix covering physical security requirements.

PIN (Personal Identification Number):
A number or code assigned to an individual and used to provide verification of identity.
Part of entity authentication on the matrix.

Policy/guideline on work station use:
Documented instructions/procedures delineating the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings, of a specific computer terminal site or type of site, dependant upon the sensitivity of the information accessed from that site.
Part of Physical safeguards to guard data integrity, confidentiality, and availability on the matrix.

Procedure for emergency access:
Documented instructions for obtaining necessary information during a crisis.
Part of access control on the matrix.

Procedures for verifying access authorizations prior to physical access:
Formal, documented policies and instructions for validating the access privileges of an entity prior to granting those privileges.
Part of physical access controls (limited access) on the matrix.

Provider:
A supplier of services as defined in section 1861(u) of the HIPAA.
A supplier of medical or other services as defined in section 1861(s) of the HIPAA.

Public key:
One of the two keys used in an asymmetric encryption system. The public key is made public, to be used in conjunction with a corresponding private key. [Stallings, 1995]

Removal from access lists:
The physical eradication of an entity's access privileges.
Part of termination procedures on the matrix.

Removal of user account(s):
The termination or deletion of an individual's access privileges to the information, services, and resources for which they currently have clearance, authorization, and need-to-know when such clearance, authorization and need-to-know no longer exists.
Part of termination procedures on the matrix.

Report procedures:
The documented formal mechanism employed to document security incidents.
Part of security incident procedures on the matrix.

Response procedures:
The documented formal rules/instructions for actions to be taken as a result of the receipt of a security incident report.
Part of security incident procedures on the matrix.

Risk analysis:
Risk analysis, a process whereby cost-effective security/control measures may be selected by balancing the costs of various security/control measures against the losses that would be expected if these measures were not in place.
Part of the security management process on the matrix.

Risk management:
Risk is the possibility of something adverse happening. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk. (NIST Pub. 800–14)
Part of the security management process on the matrix.

Role-based access control:
Role-based access control (RBAC) is an alternative to traditional access control models (e.g., discretionary or non-discretionary access control policies) that permits the specification and enforcement of enterprise-specific security policies in a way that maps more naturally to an organization's structure and business activities. With RBAC, rather than attempting to map an organization's security policy to a relatively low-level set of technical controls (typically, access control lists), each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform that role.
Part of access control on the matrix.
Part of authorization control on the matrix.

Sanction policy:
Organizations must have policies and procedures regarding disciplinary actions which are communicated to all employees, agents and contractors, for example, verbal warning, notice of disciplinary action placed in personnel files, removal of system privileges, termination of employment and contract penalties (ASTM E 1869)
In addition to enterprise sanctions, employees, agents, and contractors must be advised of civil or criminal penalties for misuse or misappropriation of health information. Employees, agents and contractors, must be made aware that violations may result in notification to law enforcement officials and regulatory, accreditation and licensure organizations. (ASTM)
Part of the security management process on the matrix.

Secure work station location:
Physical safeguards to eliminate or minimize the possibility of unauthorized access to information, for example, locating a terminal used to access sensitive information in a locked room and restricting access to that room to authorized personnel, not placing a terminal used to access patient information in any area of a doctor's office where the screen contents can be viewed from the reception area.
Part of physical safeguards to guard data integrity, confidentiality, and availability on the matrix.

Security:
Security encompasses all of the safeguards in an information system, including hardware, software, personnel policies, information practice policies, disaster preparedness, and the oversight of all these areas. The purpose of security is to protect both the system and the information it contains from unauthorized access from without and from misuse from within.
Through various security measures, a health information system can shield confidential information from unauthorized access, disclosure and misuse, thus protecting privacy of the individuals who are the subjects of the stored data. (Privacy and Health Information Systems: A Guide to Protecting Patient Confidentiality)

Security awareness training:
All employees, agents, and contractors must participate in information security awareness training programs. Based on job responsibilities, individuals may be required to attend customized education programs that focus on issues regarding use of health information and responsibilities regarding confidentiality and security. (ASTM)
Part of Physical safeguards to guard data integrity, confidentiality, and availability on the matrix.

Security configuration management:
Measures, practices and procedures for the security of information systems should be coordinated and integrated with each other and other measures, practices and procedures of the organization so as to create a coherent system of security. (OECD Guidelines, as cited in NIST Pub 800–14)
Part of administrative procedures to guard data integrity, confidentiality, and availability on the matrix.

Security incident procedures:
Formal, documented instructions for reporting security breaches.
Part of administrative procedures to guard data integrity, confidentiality and availability on the matrix.

Security management process:
A security management process encompasses the creation, administration and oversight of policies to ensure the prevention, detection, containment, and correction of security breaches. It involves risk analysis and risk management, including the establishment of accountability, management controls (policies and education), electronic controls, physical security, and penalties for the abuse and misuse of its assets, both physical and electronic.

Part of administrative procedures to guard data integrity, confidentiality and availability on the matrix.

Security policy:
The framework within which an organization establishes needed levels of information security to achieve the desired confidentiality goals. A policy is a statement of information values, protection responsibilities, and organization commitment for a system. (OTA, 1993) The American Health Information Management Association recommends that security policies apply to all employees, medical staff members, volunteers, students, faculty, independent contractors, and agents. (AHIMA, 1996c) (as cited in HISB, DRAFT GLOSSARY OF TERMS RELATED TO INFORMATION SECURITY IN HEALTH CARE INFORMATION SYSTEMS draft Glossary of Terms Related to Information Security in Health Care Information Systems)
Part of the security management process on the matrix

Security testing:
A process used to determine that the security features of a system are implemented as designed and that they are adequate for a proposed applications environment. This process includes hands-on functional testing, penetration testing, and verification. (Glossary of INFOSEC and INFOSEC Related Terms—Idaho State University)
Part of security configuration mgmt on the matrix.

Sign-in for visitors and escort, if appropriate:
Formal, documented procedure governing the reception and hosting of visitors.
Part of physical access controls (limited access) on the matrix.

Subject/object separation:
Access to a subject does not guarantee access to the objects associated with that subject.
Subject is defined as an active entity, generally in the form of a person, process, or device that causes information to flow among objects or changes the system state. Technically, a process/domain pair. (Glossary of INFOSEC and INFOSEC Related Terms—Idaho State University)
Object is defined as a passive entity that contains or receives information. Access to an object potentially implies access to the information it contains. Examples of objects are: records blocks, pages, segments, files, directories, directory trees, and programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printers, network nodes, etc. (Glossary of INFOSEC and INFOSEC Related Terms—Idaho State University)
A type of access control.

System users, including maintenance personnel, trained in security:
See Awareness training (including management).
Part of personnel security on the matrix.

Technical security mechanisms:
The processes that are put in place to guard against unauthorized access to data that is transmitted over a communications network,
A section of the matrix.

Technical security services:
The processes that are put in place (1) to protect information and (2) to control and monitor individual access to information.
A section of the matrix.

Telephone callback:
A method of authenticating the identity of the receiver and sender of information through a series of ''questions'' and ''answers'' sent back and forth establishing the identity of each. For example, when the communicating systems exchange a series of identification codes as part of the initiation of a session to exchange information, or when a host computer disconnects the initial session before the authentication is complete, and the host calls the user back to establish a session at a predetermined telephone number.
Part of Entity authentication on the matrix.

Termination procedures:
Formal, documented instructions, which include appropriate security measures, for the ending of an employee's employment, or an internal/external user's access.
Part of administrative procedures to guard data integrity, confidentiality and availability on the matrix.

Testing and revision:
(1) Testing and revision of contingency plans refers to the documented process of periodic testing to discover weaknesses in such plans and the subsequent process of revising the documentation if necessary.
Part of contingency plan on the matrix.
(2) Testing and revision of programs should be restricted to formally authorized personnel.
Part of physical access controls (limited access) on the matrix.

Time-of-day:
Access to data is restricted to certain time frames, e.g., Monday through Friday, 8:00 a.m. to 6:00 p.m.
A type of access control on the matrix.

Time-stamp:
To create a notation that indicates, at least, the correct date and time of an action, and the identity of the person that created the notation.

Token:
A physical item that's used to provide identity. Typically an electronic device that can be inserted in a door or a computer system to obtain access. (O'Reilly, 1992) (as cited in HISB, DRAFT GLOSSARY OF TERMS RELATED TO INFORMATION SECURITY IN HEALTH CARE INFORMATION SYSTEMS draft Glossary of Terms Related to Information Security in Health Care Information Systems)
Part of entity authentication on the matrix

Training:
Education concerning the vulnerabilities of the health information in an entity's possession and ways to ensure the protection of that information.
Part of administrative procedures to guard data integrity, confidentiality and availability on the matrix.

Transportability:
A signed document can be transported (over an insecure network) to another system, while maintaining the integrity of the document.
Part of digital signature on the matrix.

Turn in keys, token or cards that allow access:
Formal, documented procedure to ensure all physical items that allow a terminated employee to access a property, building, or equipment are retrieved from that employee, preferably prior to termination.
Part of termination procedures on the matrix.

Unique user identification:
The combination name/number assigned and maintained in security procedures for identifying and tracking individual user identity. (ASTM)
Part of Entity authentication on the matrix.

User authentication:
The provision of assurance of the claimed identity of an entity. (ASTM E1762–5)
Part of digital signature on the matrix.

User-based access:
A security mechanism used to grant users of a system access based upon the identity of the user.
Part of access control on the matrix.
Part of authorization control on the matrix.

User education in importance of monitoring log in success/failure, and how to report discrepancies:
Training in the user's responsibility to ensure the security of health care information.
Part of training on the matrix.

User education concerning virus protection:
Training relative to user awareness of the potential harm that can be caused by a virus, how to prevent the introduction of a virus to a computer system, and what to do if a virus is detected.
Part of training on the matrix.

User education in password management:
A type of user training in the rules to be followed in creating and changing passwords and the need to keep them confidential.
Part of training on the matrix.

Virus checking:
A computer program that identifies and disables:
(1) another ''virus'' computer program, typically hidden, that attaches itself to other programs and has the ability to replicate. (Unchecked virus programs result in undesired side effects generally unanticipated by the user.)
(2) A type of programmed threat. A code fragment (not an independent program) that reproduces by attaching to another program. It may damage data directly, or it may degrade system performance by taking over system resources which are then not available to authorized users. (O'Reilly, 1992, as cited in HISB, DRAFT GLOSSARY OF TERMS RELATED TO INFORMATION SECURITY IN HEALTH CARE INFORMATION SYSTEMS draft Glossary of Terms Related to Information

Security in Health Care Information Systems)

(3) Code embedded within a program that causes a copy of itself to be inserted in one or more other programs. In addition to propagation, the virus usually performs some unwanted function. (Stallings, 1995, as cited in HISB, DRAFT GLOSSARY OF TERMS RELATED TO INFORMATION SECURITY IN HEALTH CARE INFORMATION SYSTEMS draft Glossary of Terms Related to Information Security in Health Care Information Systems)

Part of security configuration mgmt on the matrix.

Acronyms

ABA American Bar Association
ADA American Dental Association
ANSI American National Standards Institute
AHIMA American Health Information Management Association
ASTM American Society for Testing and Materials
CDT Center for Democracy & Technology
CEN Central European Nations
CORBA Common Object Request Broker
CPRI Computer-based Patient Record Institute
DAC Discretionary Access Control
DEA Data Encryption Algorithm
EDI Electronic Data Interchange
EHNAC Electronic Healthcare Network Accreditation Commission
FDA Food and Drug Administration
HISB Health Care Informatics Standards Board
ISO International Organization for Standardization
MAC Mandatory Access Control
NCSC National Computer Security Center
NCQA National Council for Quality Assurance
NCVHS National Committee on Vital and Health Statistics
NUBC National Uniform Billing Committee
NUCC National Uniform Claim Committee
PGP Pretty Good Privacy
PIN Personal Identification Number
NIST National Institutes of Standards and Technology
SDO Standards Development Organization
WEDI Workgroup for Electronic Data Interchange

Bibliography

ABA, Digital Signature Guidelines.
ANSI, ASC X12.58, Security Structures, June, 1997.
ASTM, E1762–95, Standard Guide for Electronic Authentication of Health Care Information. ASTM Committee E–31 on Computerized Systems, Subcommittee E31.20 on Authentication. West Conshohocken, PA, October 10, 1995.
ASTM, A Security Framework for Healthcare Information. ASTM Committee E–31 on Computerized Systems, Subcommittee E31.20 on Authentication. West Conshohocken, PA, February 11, 1997.
EDI Security, Control, and Audit, Marcells, Albert J. & Chan, Sally. Artech House, 685 Canton Street, Norwood, MA 01602, 1993.
FDA, Electronic Record; Electronic Signatures; Final Rule.
For the Record—Protecting Electronic Health Information, Computer Science and Telecommunications Board, NRC, National Academy Press, 2102 Constitution Avenue, NW, Box 285, Washington, DC, 20055, 1997.
Glossary of INFOSEC and INFOSEC Related Terms, Version 6. Schou, Corey D., Center for Decision Support, Idaho State University. August, 1996
HISB, DRAFT GLOSSARY OF TERMS RELATED TO INFORMATION SECURITY IN HEALTH CARE INFORMATION SYSTEMS Glossary of Terms Related to Information Security in Health Care Information Systems draft, 1997
NCSC, Glossary of Computer Security Terms, October 21, 1988.
NIST Pub 800–14, ''Generally Accepted Principles and Practices for Securing Information Technology Systems'', Swanson, Marianne, & Guttman, Barbara, September, 1996. PGP, Inc., Cryptology Reference Chart, August, 1997
Privacy and Health Information Systems: A Guide to Protecting Patient Confidentiality, Goldman, Janlori & Mulligan, Deirdre, CDT, 1996.

Addendum 3

HIPAA SECURITY MATRIX—mapping

Please Note: While we have attempted to categorize security requirements for ease of understanding and reading clarity, there are overlapping areas on the matrix in which the same requirements are restated in a slightly different context.

ADMINISTRATIVE PROCEDURES TO GUARD DATA INTEGRITY, CONFIDENTIALITY, AND AVAILABILITY

Requirement	Implementation	Mapped standards
Certification		47.
Chain of trust partner agreement		12, 47.
Contingency plan (all listed implementation features must be implemented).	Applications and data criticality analysis	17, 47, 53.
	Data backup plan	12, 17, 47.
	Disaster recovery plan	12, 17, 47, 53.
	Emergency mode operation plan	47, 53.
	Testing and revision	12, 17, 47.
Formal mechanism for processing records		12, 17.
Information access control (all listed implementation features must be implemented).	Access authorization	12, 17, 47, 53.
	Access establishment	17, 47, 53.
	Access modification	12, 17, 47, 53.
Internal audit		12, 17, 43, 44, 47.
Personnel security (all listed implementation features must be implemented)	Assure supervision of maintenance personnel by authorized, knowledgeable person.	17, 47.
	Maintainance of record of access authorizations.	12, 17, 47.
	Operating, and in some cases, maintenance personnel have proper access authorization.	17, 47.
	Personnel clearance procedure	17, 47.
	Personnel security policy/procedure	17, 47, 53.
	System users, including maintenance personnel, trained in security.	12, 17, 47, 53.
Security configuration mgmt. (all listed implementation features must be implemented).	Documentation	12, 17, 47, 53.
	Hardware/software installation & maintenance review and testing for security features.	12, 17, 47.
	Inventory	12, 17.
	Security testing	12, 17, 47.
	Virus checking	12, 17, 47, 53.
Security incident procedures (all listed implementation features must be implemented).	Report procedures	12, 17, 47.
	Response procedures	17, 47.