

Document Title	Background Paper – Health Information Security Standards Framework and Glossary of Terms
Source	Brendan Seaton – Canada Ian Shepherd - UK
Action Required	For review and discussion at 2 nd WG4 meeting, 1999-04-12

Convenor of ISO/TC 215/WG 4	Technical Secretary of WG 4
Gunnar Klein, HSS	Nagaaki Ohyama, Tokyo Institute of Technology Imaging Science and Engineering Laboratory
Box 70 487, S-107 26 Stockholm, Sweden	4259 Nagatsuta, Midori-ku, Yokohama 226-8503, Japan
E-mail: wg4.isotc215@hss.se	E-mail: wg4kita@medis.or.jp
Phone + 46-8-81 52 52, Fax +46-8-702 49 15	Phone: +81-45-924-5177, Fax: +81-45-924-5175
Local Secretary: Lena Naslund +46-8-702 49 17	Assistant of Secretary of WG4: Kouichi Kita, Phone: +81-45-924-5186, Fax: +81-45-924-5175

Table of Contents

1	PURPOSE.....	1
2	WG 4 SCOPE STATEMENT	1
3	FRAMEWORK FOR SECURITY STANDARDS	1
3.1	TECHNICAL COUNTERMEASURES	3
3.2	SYSTEMATIC COUNTERMEASURES.....	3
3.3	INSTITUTIONAL COUNTERMEASURES	3
4	WG 4 DOCUMENTS	3
4.1	BACKGROUND PAPERS AND TECHNICAL REPORTS.....	4
4.2	GUIDELINES	5
4.3	STANDARDS.....	5
5	GLOSSARY OF TERMS	5
	ANNEX 1 - GLOSSARY OF TERMS.....	7

**Background Paper
Health Information Security Standards Framework
and Glossary of Terms**

1 Purpose

This Background Paper has been prepared to assist ISO/TC 215/WG 4 in arriving at a common framework for the development of health information security standards, and to present a glossary of terms that can be used to ensure consistency of definitions in the preparation of technical documents for the Working Group.

2 WG 4 Scope Statement

At the first meeting of Working Group 4 the following scope statement was adopted:

Defining standards for technical measures to ensure the confidentiality, availability and integrity of health information, and also accountability for users, as well as guidelines for security management in healthcare.¹

3 Framework for Security Standards

The Report from the ad hoc group preparing the Security Working Group² identified that the security of communicated and stored information requires countermeasures on three levels:

¹ISO/TC 215/WG 4/N9, 1999-03-08, p. 5

²ISO/TC 215/WG 4/N2, 1998-08-25, p. 2

- Technical
- Systemic (organisational)
- Institutional (legislative and ethical)

The standards developed by the Working Group would deal with the first two levels, but the Working Group and people implementing the standards should be aware of legislative and regulatory aspects. The standards should enable flexibility in implementation to reflect local professional agreements and practice.

3.1 Technical Countermeasures

Technical countermeasures will deal primarily with the specifications required to ensure interoperability between health information systems, connection with health information networks and with the technical measures required to protect the confidentiality, availability and integrity of health information. Examples of technical countermeasures include secure communications protocols, encryption algorithms, access controls, and security architectures.

3.2 Systemic Countermeasures

Systemic countermeasures will deal primarily with the processes and procedures used by health service professionals and organizations to protect the confidentiality, availability and integrity of health information. Examples of systemic countermeasures include security management guidelines, security training for personnel, personal privacy protection, and threat and risk assessment.

3.3 Institutional Countermeasures

Institutional or legislative countermeasures are beyond the scope of WG 4. However, legislation in many countries, and agreements between countries, will influence the development of technical and systemic security countermeasures and standards. WG 4 must consider the impacts of legislative requirements when defining the need for security standards, and when determining the appropriate security standard solution.

4 WG 4 Documents

Working Group 4 will be preparing a variety of documents that will guide health service professionals and organizations in the development of their information security programs. These documents will generally fall into one of the three following categories:

- Background papers and technical reports
- Guidelines
- Standards

4.1 Background Papers and Technical Reports

Background papers and technical reports will be prepared to support the work of the WG 4, but could be used as reference material by health service professionals and organizations. These documents will be used as background research for the development of standards and guidelines. Such documents would include a thorough analysis of a subject area, and could recommend measures that may be adopted as standards and guidelines.

4.2 Guidelines

Guidelines are voluntary measures that could be adopted by health service professionals and organizations or regulatory bodies. Guidelines define “best practice” with respect to health information security, but their implementation may be discretionary depending on local requirements or circumstances. Guidelines would be most common in the area of systemic countermeasures.

4.3 Standards

Standards are mandatory measures that are required to ensure the interoperability of information systems and networks, and minimum requirements for information security. Failure to adopt approved standards would compromise the security of health information or the effective operation of health information systems. Standards would be most common in the area of technical countermeasures.

5 Glossary of Terms

To reduce the possibility of misinterpretation of WG 4 documents, a glossary of terms with standard definitions is required. The glossary found in Annex 1 is proposed as the standard glossary for all WG 4 documents. Terms and definitions have been drawn from the following sources:

Source	Abbreviation in Glossary
Security Framework for Health Information, ASTM, PS 101-97, March 1998	ASTM
Medical Informatics - Security Categorisation and Protection for Healthcare Information Systems, CEN, ENV 12924, November 1997	CEN
Working Group 3: Privacy, Confidentiality, Data Integrity and Security - Background Document (Revised), Canadian Institute for Health Information, 1997	CIHI

Privacy and Security Guidelines for Health Information Systems, Canadian Organization for the Advancement of Computers in Health, 1995	COACH
Standard Guide for EDI (HL7) Communication Security, B. Blobel, Otto-von-Guericke University Magdeburg, HL7 Germany	HL7
Information Technology - Vocabulary - Part 8: Security, ISO/IEC JTC 1, ISO 2382-8, Draft - December 1996	ISO/IEC 2382-8
NHS IM&T Security Manual, V1.0, February 1996	NHS

It is recommended that WG4 establish a standing sub-committee to review the definitions identified in Annex 1, and to maintain the glossary as new terms and definitions are added, or obsolete terms and definitions are modified or deleted.

Annex 1 - Glossary of Terms

DRAFT

Glossary of Terms

DRAFT

TERM	DEFINITION	SOURCE
Aborted connection	A disconnection that does not follow established procedures. NOTE: an aborted connection may enable other entities to gain unauthorized access	ISO/IEC 2382-08
Access	The process of obtaining data from, or placing data into a computer system or storage device	COACH
Access category	A category to which entities may be assigned, based on the resources that the entity is authorized to use	ISO/IEC 2382-08
Access control	A means of ensuring that the resources of a data processing system can be accessed only by authorized entities in authorized ways	ISO/IEC 2382-08
Access control list	A list of entities, together with their access rights, that are authorized to access a resource	ISO/IEC 2382-08
Access level	The level of authority required from an entity to access a protected resource. Example: the authority to access information at a particular security level	ISO/IEC 2382-08
Access list	A list or entities, together with their access rights, that are authorized to access a resource	ISO/IEC 2382-08
Access period	A period of time during which specified access rights prevail	ISO/IEC 2382-08
Access permission	All of a subject's access rights with respect to some object	ISO/IEC 2382-08
Access right	Permission for a subject to access a particular object for a specific type of operation	ISO/IEC 2382-08
Access type	A type of operation specified by an access right. Examples :read, write, execute, append, modify, delete, create	ISO/IEC 2382-08
Accountability	The property that ensures that the actions of an entity may be traced uniquely to that entity	ISO/IEC 2382-08
Accreditation (in computer security)	The authorization and approval, granted by a designated authority to a data processing system, computer network, organization, or individual, to process sensitive information or data	ISO/IEC 2382-08
Active threat	A threat of deliberate unauthorized change to the state of a data processing system. Examples: modification of messages, insertion of spurious messages, masquerade, denial of service.	ISO/IEC 2382-08
Active wiretapping	Wiretapping with the purpose to modify or insert data	ISO/IEC 2382-08
Administrative security	Administrative measures for computer security. NOTE: those measures may be operational and accountability procedures, procedures of investigation breaches in security, and reviewing audit trails.	ISO/IEC 2382-08
Aggregation	Acquisition of sensitive information by collecting and correlating information of lesser sensitivity	ISO/IEC 2382-08
Algorithm	A clearly specified mathematical process for computation; a set of rules which, if followed, will give a prescribed result	ASTM
Analytical attack	An attempt to break a code or to find a key using analytical methods. Examples: statistical analysis of patterns, discovering flaws in an	ISO/IEC 2382-08

	encryption algorithm	
Anonymous	With respect to data, the condition of not being able to identify data or information with an individual person	COACH
Anti-virus program	A program designed to detect viruses and possibly to suggest or take corrective action	ISO/IEC 2382-08
<to> archive	To store backup files and any associated journals, usually for a given period of time	ISO/IEC 2382-08
Archived file	A file for which an archive file exists	ISO/IEC 2382-08
Archive file	A file set aside for later research of verification, for security, or for any other purpose	ISO/IEC 2382-08
Archiving	The process of saving data for later reference or use	COACH
Asset	Any item that has value	COACH
Asset owner	Individual or organization having responsibility for specified information asset(s) and for the maintenance of appropriate security measures	NHS
Asymmetric cryptography	Cryptography in which a public key and a corresponding private key are used for encryption and decryption	ISO/IEC 2382-08
Attack	An attempt to violate computer security. Examples: malicious logic, wiretapping	ISO/IEC 2382-08
Audit	An independent examination of a work product or set of work products to assess compliance with specifications, standards, contractual agreements, or other criteria	COACH
Audit trail (in computer security)	Data collected and for the potential use in a security audit	ISO/IEC 2382-08
Authentication	The act of verifying the claimed identity of an entity	ISO/IEC 2382-08
Authentication exchange	A method intended to ensure the identity of an entity by means of an information exchange	ISO/IEC 2382-08
Authentication information	Information used to establish the validity of a claimed identity	ISO/IEC 2382-08
Authentication token	A device allocated to an entity to assist the authentication of that entity	CEN
Authorization	The granting of rights, which includes the granting of access based on access rights	ISO/IEC 2382-08
Availability (in computer security)	The property of data or of resources being accessible and usable on demand by an authorized entity	ISO/IEC 2382-08
Backup file	A file made for possible later data restoration. Example: a copy of a file preserved at an alternate site	ISO/IEC 2382-08
Backup procedure	A procedure to provide for data restoration in case of a failure or a disaster. Example: making backup files	ISO/IEC 2382-08
Backward recovery	The data reconstitution of an earlier version of data by using a later version and data recorded in a journal	ISO/IEC 2382-08
Bacterium	A program that propagates itself by electronic mail to everyone in each recipient's distribution list	ISO/IEC 2382-08
Bad sectoring	A technique for copy protection in which bad sectors are intentionally written on a diskette	ISO/IEC 2382-08
Between-the-lines entry	Access obtained through active wiretapping by an unauthorized user to a momentarily inactive transmission channel connected to a legitimate user resource	ISO/IEC 2382-08
Biometric	Pertaining to the use of specific attributes that reflect unique personal characteristics, such as a fingerprint, an eye blood-vessel print, or a voice print, to validate the identity of entities	ISO/IEC 2382-08

Biometric authentication technology	Technology which uses some human biological feature (such as a fingerprint or voice print) to uniquely identify an individual	CIHI
Breach	The circumvention or disablement of some element of computer security, with or without detection, which could result in a penetration of the data processing system	ISO/IEC 2382-08
Brute-force attack	A trial-and-error attempt to violate computer security by trying possible values of passwords or keys. NOTE: contrast with analytical attack	ISO/IEC 2382-08
Call-back	A procedure in which a data processing system identifies a calling terminal, disconnects the call, and dials the calling terminal to authenticate the calling terminal	ISO/IEC 2382-08
Capability (in computer security)	A representation of the address of an object and of a set of authorized access types	ISO/IEC 2382-08
Capability list	A list associated with a subject that identifies all of the subject's access types of all objects. Example: a list associated with a process that identifies all of its access types for all files and other protected resources	ISO/IEC 2382-08
CAS (abbreviation of Controlled Access System)	A means of automating physical access control. Example: the use of magnetic striped badges, smart cards, biometric readers.	ISO/IEC 2382-08
Certification (in computer security)	Procedure by which a third party gives assurance that all or part of a data processing system conforms to security requirements	ISO/IEC 2382-08
Chain letter	A program that propagates itself by electronic mail to everyone in each recipient's distribution list	ISO/IEC 2382-08
Checking code	Machine instructions that read part of a diskette to determine whether it is an unauthorized copy	ISO/IEC 2382-08
Chosen-plaintext attack	An analytical attack in which a cryptanalyst can submit an unlimited number of plaintext messages examine the corresponding ciphertext	ISO/IEC 2382-08
Ciphersystem	The documents, devices, equipment, and associated techniques that are used together to provide a means of encryption or decryption	ISO/IEC 2382-08
Ciphertext	Data produced through the use of encryption, the semantic content of which is not available without the use of cryptographic techniques [ISO 7498-2 m]	ISO/IEC 2382-08
Ciphertext-only attack	An analytical attack in which a cryptanalyst possesses only ciphertext	ISO/IEC 2382-08
Clearance	Permission granted to an individual to access information at or below a particular security level	ISO/IEC 2382-08
Clearing (in computer security)	Overwriting classified data on a data medium that has a particular security classification and security category, so that this data medium may be reused for writing at the same security classification and security category	ISO/IEC 2382-08
Cleartext	Data, the semantic content of which is available without using cryptographic techniques [ISO 7498-2 m]	ISO/IEC 2382-08
Closed-security environment	An environment in which special attention is paid (in the form of authorizations, security clearances, configuration controls, etc.) to protect data and resources from accidental or malicious acts	ISO/IEC 2382-08
Cold site	An alternative facility with at least the equipment necessary to support the installation and operation of a data processing system in the event of disaster	ISO/IEC 2382-08
Collection	The process of gathering data from a number of individuals or	COACH

	sources	
Communication	The process of transmitting data or information from one point to another	COACH
Communications security	Computer security applied to data communication	ISO/IEC 2382-08
Compartmentalization	A division of data into small, isolated blocks for the purpose of reducing risk. Example: the isolation of the operating system, application software, and files from one another in a storage device in order to provide protection against unauthorized or concurrent access	ISO/IEC 2382-08
Compromise	A violation of computer security whereby programs or data may have been modified, destroyed, or made available to unauthorized entities	ISO/IEC 2382-08
Compromising emanation	Signals that are unintentionally emitted and that, if intercepted and analyzed, may reveal sensitive information being processed or transmitted. Examples: acoustic emanation, electromagnetic emanation.	ISO/IEC 2382-08
COMPUSEC (abbreviation/US)	The protection of data and resources from accidental or malicious acts, usually by taking appropriate actions. NOTE: those acts may be loss or unauthorized modification, destruction, access, disclosure, or acquisition	ISO/IEC 2382-08
Computer abuse	A willful or negligent unauthorized activity that affects the computer security of a data processing system	ISO/IEC 2382-08
Computer crime	A crime committed with the aid of, or directly involving, a data processing system or network. NOTE: this is an improved version of the definition in ISO/IEC 2382-1:1993	ISO/IEC 2382-08
Computer fraud	A fraud committed with the aid of, or directly involving, a data processing system or network	ISO/IEC 2382-08
Computer program	A combination of computer instructions and data definitions that enable computer hardware to perform computational or control functions	COACH
Computer security (abbr. COMPUSEC)	The protection of data and resources from accidental or malicious acts, usually by taking appropriate actions. NOTE: those acts may be loss or unauthorized modification, destruction, access, disclosure, or acquisition.	ISO/IEC 2382-08
Computer-system audit	An examination of the procedures used in a data processing system to evaluate their effectiveness and correctness, and to recommend improvements	ISO/IEC 2382-08
Confidentiality	A property of data that indicates the extent to which these data have not been made available or disclosed to unauthorized individuals, processes, or other entities	ISO/IEC 2382-08
Consent	Voluntary agreement with what is being done or proposed (express or implied)	CIHI
Contamination	The introduction of data of one security classification or security category into data of a lower security classification or different security category	ISO/IEC 2382-08
Contingency plan	A plan for backup procedures, emergency responses, and post-disaster recovery	ISO/IEC 2382-08
Contingency procedure	A procedure that is an alternative to the normal path of a process if an unusual but anticipated situation occurs	ISO/IEC 2382-08
Controlled access system (CAS-	A means of automating physical access control	ISO/IEC 2382-08

abbreviation)		
Copy protection	The use of special techniques to detect or prevent the unauthorized copying of data, software, or firmware	ISO/IEC 2382-08
Countermeasure	An action, device, procedure, technique, or other measure that is designed to minimize vulnerability	ISO/IEC 2382-08
Covert channel	A transmission channel that may be used to transfer data in a manner that violates security policy	ISO/IEC 2382-08
CRAMM	The CCTA risk analysis and management method	NHS
Credentials	Data that are transferred to establish the claimed identity of an entity	ISO/IEC 2382-08
Criticality	The degree of importance assigned to information denoting its need for protection against integrity and availability security breaches	CEN
Cryptanalysis	The analysis of a cryptographic system, its inputs or outputs, or both, to derive sensitive information, including plaintext	ISO/IEC 2382-08
Cryptanalytical attack	An attempt to break a code or to find a key using analytical methods. Examples: statistical analysis of patterns; discovering flows in an encryption algorithm	ISO/IEC 2382-08
Cryptographic check value	Information which is derived by performing a cryptographic transformation on data	HL7
Cryptographic system	The documents, devices, equipment, and associated techniques that are used together to provide a means of encryption or decryption	ISO/IEC 2382-08
Cryptography	The discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification	ISO/IEC 2382-08
Cryptosystem	The documents, devices, equipment, and associated techniques that are used together to provide a means of encryption or decryption	ISO/IEC 2382-08
Data	A representation of facts, concepts, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automatic means	COACH
Data authentication	A process used to verify data integrity. Examples: verification that data received are identical to data sent, verification that a program is not infected by a virus. NOTE: not to be confused with authentication	ISO/IEC 2382-08
Database	A collection of logical related data stored together in one or more computerized files	COACH
Data corruption	An accidental or intentional violation of data integrity	ISO/IEC 2382-08
Data integrity	The property of data whose accuracy and consistency are preserved regardless of changes made	ISO/IEC 2382-08
Data (or record) linkage	A method of assembling information contained in two or more different files or records to relate significant health and other events for the same individual, organization, community, or other unit of analysis	CIHI
Data origin authentication	A principal claiming to be the originator of some data includes its identity along with that data glued together using the integrity service	HL7
Data protection	The implementation of administrative, technical, or physical measures to guard against the unauthorized access to data. NOTE: this is an improved version of the definition in ISO/IEC 2382-1:1993	ISO/IEC 2382-08
Data reconstitution	A method of data restoration by assembling data from components available in alternative sources	ISO/IEC 2382-08
Data reconstruction	A method of data restoration by analyzing original sources	ISO/IEC 2382-08

Data restoration	The act of regenerating data that have been lost or contaminated. NOTE: methods include copying data from archive, data reconstitution from alternative sources, or data reconstruction from source data	ISO/IEC 2382-08
Data security	Computer security applied to data	ISO/IEC 2382-08
Data user	Data user means a person who holds data, and a person “holds” data if: <ul style="list-style-type: none"> • The data form part of a collection of data processed or intended to be processed by or on behalf of the person, and • That person (either alone or jointly or in common with other persons) controls the contents and use of the data comprised in the collection, and • The data are in the form in which they have been or are intended to be processed and with a view to being further so processed on a subsequent occasion 	NHS
Data validation	A process used to determine if data are accurate, complete, or meet specified criteria. NOTE: data validation may include format checks, completeness checks, check key tests, reasonableness checks, and limit checks	ISO/IEC 2382-08
Decipherment	The process of obtaining, from a ciphertext, the original corresponding data. NOTE: a ciphertext may be encrypted a second time, in which case a single decryption does not produce the original plaintext	ISO/IEC 2382-08
Decryption	The process of obtaining, from a ciphertext, the original corresponding data. NOTE: a ciphertext may be encrypted a second time, in which case a single decryption does not produce the original plaintext	ISO/IEC 2382-08
Denial of service	The prevention of authorized access to resources or the delaying of time-critical operations	ISO/IEC 2382-08
Destruction	The process of rendering an asset completely unusable	COACH
Dial-back	A procedure in which a data processing system identifies a calling terminal, disconnects the call, and dials the calling terminal to authenticate the calling terminal	ISO/IEC 2382-08
Digital envelope	Data appended to a message, that allow the intended recipient to verify the content of the message	ISO/IEC 2382-08
Digital signature	Data appended to a message, that allow the recipient of the message to ensure the source and integrity of the message	ISO/IEC 2382-08
Disaster recovery plan	A plan for backup procedures, emergency response, and post-disaster recovery	ISO/IEC 2382-08
Disclosure	A violation of computer security whereby data have been made available to unauthorized entities	ISO/IEC 2382-08
Eavesdropping	The unauthorized interception of information-bearing emanations	ISO/IEC 2382-08
Electronic mail	The generation, transmission, and display of correspondence and documents by electronic means	ISO/IEC 2382-08
Employee	An individual employed by an Health Service Enterprise	COACH
Encipherment	The cryptographic transformation of data [ISO 7498-2 m]. Notes: <ol style="list-style-type: none"> 1. The result of encryption is ciphertext 2. The reverse process is called decryption 3. See also: public key cryptography, symmetric cryptography, irreversible encryption 	ISO/IEC 2382-08
Encryption	The cryptographic transformation of data [ISO 7498-2 m]. Notes:	ISO/IEC 2382-08

	1 The result of encryption is ciphertext 2. The reverse process is called decryption 3. See also: public key cryptography, symmetric cryptography, irreversible encryption	
Encryption key	A binary number used to transform plain text into cipher text	ASTM
Entrapment	The deliberate planting of apparent flaws in a data processing system for the purpose of detecting attempted penetrations or for confusing an intruder about which flaws to exploit	ISO/IEC 2382-08
Exhaustive attack	A trial-and-error attempt to violate computer security by trying possible values of passwords or keys. NOTE: contrast with analytical attack	ISO/IEC 2382-08
Exposure	The potential compromise associated with an attack exploiting a corresponding vulnerability	ISO/IEC 2382-08
Extra sector	A sector that is written on a diskette track in excess of the standard number of sectors, as part of a method of copy protection	ISO/IEC 2382-08
Extra track	A track that is written on a diskette in excess of the standard number of tracks, a part of a method of copy protection	ISO/IEC 2382-08
Failsafe (in computer security)	Pertaining to avoidance of compromise in the event of a failure	ISO/IEC 2382-08
Failure access	An unauthorized and usually inadvertent access to data in a data processing system, resulting from a failure of hardware or software	ISO/IEC 2382-08
Fake sector	A sector consisting of a header but no data, used in large numbers on a diskette to cause an unauthorized copying program to fail to copy the diskette	ISO/IEC 2382-08
File protection	The implementation of appropriate administrative, technical, or physical means to guard against the unauthorized access to, modification of, or deletion of a file	ISO/IEC 2382-08
Firewall	A filter between a network of trusted computers and other networks	CIHI
Flaw (in computer security)	An error of commission, an omission, or an oversight that allows protection mechanisms to be bypassed or disabled	ISO/IEC 2382-08
Flooding	Accidental or intentional insertion of a large volume of data resulting in denial of service	ISO/IEC 2382-08
Forward recovery	The data reconstitution of a later version of data by using an earlier version and data recorded in a journal	ISO/IEC 2382-08
Gateway	A computer system or other device that acts as a translator between two systems that do not use the same communications protocols, data formatting, structures, languages, or architecture, or a combination thereof	ASTM
Guard (in computer security)	A functional unit that provides a security filter between two data processing systems operating at different security levels or between a user terminal and a database to filter out data that the user is not authorized to access	ISO/IEC 2382-08
Hardware	Physical equipment used to process, store, or transit computer programs or data	COACH
Health care data	Data which are input, stored, processed or output by the automated information system which support the business functions of the Health Care Establishment. These data may relate to person identifiable records or may be part of an administrative system where persons are not identified	CEN
Health care provider	Any individual employed or engaged in the direct delivery of health services or products to patients	COACH

Health data	Facts that apply to the health status of an individual and/or to the treatment or care provided to that individual	COACH
Health service enterprise	Any organization engaged in the planning funding, management, manufacture or delivery of health services and products	COACH
Hot site	A fully equipped computer center that provides an immediate alternative data processing capability for use in the event of a disaster	ISO/IEC 2382-08
Identification	Unique name of a principal	HL7
Identity authentication	The performance of tests to enable a data processing system to recognize entities	ISO/IEC 2382-08
Identity validation	The performance of tests to enable a data processing system to recognize entities	ISO/IEC 2382-08
Identity token	A device used for identity authentication. Examples: smart card, metal key	ISO/IEC 2382-08
Impact	The embarrassment, harm, financial loss, legal or other damage which could occur in consequence to a particular security breach	CEN
Information	The meaning that humans assign to data by means of known conventions that are applied to the data	COACH
Information security	Protection of information for: <ul style="list-style-type: none"> • Confidentiality • Integrity • Availability 	NHS
Information system	A mechanism used for acquiring, filing, storing and retrieving an organized body of knowledge	COACH
Integrity	The property that data has not been altered or destroyed in an unauthorized manner	CEN
Irreversible encryption	Encryption that produces ciphertext from which the original data cannot be reproduced. NOTE: irreversible encryption is useful in authentication. For example, a password might be irreversibly encrypted and the resulting ciphertext stored. A password presented later would be irreversibly encrypted identically and the two strings of ciphertext compared. If they are identical, the presented password is correct	ISO/IEC 2382-08
Irreversible encryption	Encryption that produces ciphertext from which the original data cannot be reproduced. NOTE: irreversible encryption is useful in authentication. For example, a password might be irreversibly encrypted and the resulting ciphertext stored. A password presented later would be irreversibly encrypted identically and the two strings of ciphertext compared. If they are identical, the presented password is correct	ISO/IEC 2382-08
Key (in computer security)	A variable-length bit string that controls the operations of encryption or decryption	ISO/IEC 2382-08
Keystroke verification	The determination of the accuracy of data entry by the re-entry of the same data through a keyboard	ISO/IEC 2382-08
Known-plaintext attack	An analytical attack in which a cryptanalyst possesses a substantial quantity of corresponding plaintext and ciphertext	ISO/IEC 2382-08
LAN	Acronym for Local Area Network	COACH
Linkage (in computer security)	The purposeful combination of data or information from one data processing system with data or information from another system to	ISO/IEC 2382-08

	derive protected information	
Logical access control	The use of information-related mechanisms to provide access control. Example: the use of a password	ISO/IEC 2382-08
Logic bomb	Malicious logic that causes damage to a data processing system when triggered by some specific system condition	ISO/IEC 2382-08
Loss	A quantitative measure of harm or deprivation resulting from a compromise	ISO/IEC 2382-08
MAC (abbreviation of Message Authentication Code)	A bit string that is a function of both data (either plaintext or ciphertext) and a secret key, and that is attached to the data in order to allow data authentication. NOTE :the function used to generate the message authentication code must be a one-way function.	ISO/IEC 2382-08
Maintenance	(1)The process of modifying a software system or component after delivery to correct faults, improve performance or other attributes, or adapt to a changed environment. (2)The process of retaining a hardware system or component in, or restoring it to, a state in which it can perform its required functions	COACH
Maintenance hook	A trapdoor in software that allows easy maintenance and development of additional features and that may allow entry into the program at unusual points or without the usual checks	ISO/IEC 2382-08
Malicious logic	A program implemented in hardware, firmware, or software, and whose purpose is to perform some unauthorized or harmful action. Examples: a logic bomb, a Trojan horse, a virus, a worm	ISO/IEC 2382-08
Manipulation detection	A procedure that is used to detect whether data have been modified, either accidentally or intentionally	ISO/IEC 2382-08
Manipulation detection code	A bit string that is a function of data that are attached to them in order to allow manipulation detection NOTES: 1. The resulting message (data plus MDC) is then encrypted in order to achieve secrecy or data authentication 2. The function used to generate the MDC must be public	ISO/IEC 2382-08
Masquerade	The pretence by an entity to be a different entity in order to gain unauthorized access	ISO/IEC 2382-08
MDC (abbreviation of Manipulation/Modification Detection Code)	A bit string that is a function of data that are attached to them in order to allow manipulation detection. NOTES: 1. The resulting message (data plus MDC) is then encrypted in order to achieve secrecy or data authentication. 2. The function used to generate the MDC must be public.	ISO/IEC 2382-08
Message authentication	Verification that a message was sent intact, unchanged and by the purported originator to the intended recipient	ISO/IEC 2382-08
Message authentication code (MAC)	A bit string that is a function of both data (either plaintext or ciphertext) and a secret key, and that is attached to the data in order to allow data authentication. NOTE :the function used to generate the message authentication code must be a one-way function	ISO/IEC 2382-08
Microdata	The most detailed level of data provided by data suppliers or respondents, which may often contain sensitive information	CIHI
Minimum privilege	Restriction of the access rights of a subject to only those rights that are necessary for the execution of authorized tasks	ISO/IEC 2382-08
Modification	The process of changing the contents or logical structure of a database or program	COACH
Modification	A procedure that is used to detect whether data have been modified,	ISO/IEC 2382-08

detection	either accidentally or intentionally	
Modification detection code	A bit string that is a function of data that are attached to them in order to allow manipulation detection NOTES: 1. The resulting message (data plus MDC) is then encrypted in order to achieve secrecy or data authentication. 2. The function used to generate the MDC must be public	ISO/IEC 2382-08
Multilevel device	A functional unit that can simultaneously process data of two or more security levels without risk of compromising computer security	ISO/IEC 2382-08
Mutual suspicion	The relationship between interacting entities in which neither entity relies upon the other entity to function correctly or securely with respect to some property	ISO/IEC 2382-08
Need-to-know	A legitimate requirement of a prospective recipient of data to know, to access, or to possess any sensitive information represented by these data	ISO/IEC 2382-08
Network weaving	A penetration technique in which different communication networks are used to gain access to a data processing system to avoid detection and trace-back	ISO/IEC 2382-08
Non-repudiation	This service provides proof of the integrity and origin of data (both in an unforgeable relationship) which can be verified by any party	ASTM
Non-repudiation of origin	The principal receiving some data claims to know the data originator so that the sender cannot later falsely deny having sent the data. The integrity service is needed for establishment	HL7
Non-repudiation of receipt	The principal sending some data claims to know that this data has been successfully reached its intended receiver. The integrity service is needed for establishment	HL7
Notarization	The registration of data with a trusted third party that allows the later assurance of the accuracy of the data's characteristics such as content, origin, time and delivery	ISO/IEC 2382-08
Object (in computer security)	An entity to which access is controlled. Examples: a file, a program, an area of main storage; a person about whom data are collected and maintained	ISO/IEC 2382-08
Offset track	A track written at a nonstandard position on a diskette as part of a method of copy protection	ISO/IEC 2382-08
One-way encryption	Encryption that produces ciphertext from which the original data cannot be reproduced. NOTE: irreversible encryption is useful in authentication. For example, a password might be irreversibly encrypted and the resulting ciphertext stored. A password presented later would be irreversibly encrypted identically and the two strings of ciphertext compared. If they are identical, the presented password is correct.	ISO/IEC 2382-08
Open-security environment	An environment in which protection of data and resources from accidental or malicious acts is achieved through normal operational procedures	ISO/IEC 2382-08
Padlocking	The use of special techniques to protect data or software against unauthorized copying	ISO/IEC 2382-08
Passive threat	A threat of disclosure of information without changing the state of a data processing system. Example: the recovery of sensitive information through the interception of data transmission	ISO/IEC 2382-08
Passive wiretapping	Wiretapping limited to obtaining data	ISO/IEC 2382-08
Password	A character string that is used as authentication information	ISO/IEC 2382-08

Patient	Any individual who receives a health product or service from a healthcare provider or health service enterprise. Often referred to as client by some health service organizations	COACH
Penetration	Unauthorized access to a data processing system	ISO/IEC 2382-08
Penetration testing	Examining the functions of a data processing system to find a means of circumventing computer security	ISO/IEC 2382-08
Personal data	Data consisting of information which relates to a living individual who can be identified from that information (or from that and other information in the possession of the Data User), including any expression of opinion about the individual but not any indication of the intentions of the Data User in respect of that individual	NHS
Personal health data	This is data as to the physical or mental health of an individual that is: <ul style="list-style-type: none"> • Held by a health professional • Or • Not held by a health professional but was first recorded by or for a health professional 	NHS
Personal/person identifiable information	Information about the characteristics or activities of an identifiable natural person, including information about individuals who may not be explicitly identified, but whose identity could be inferred from elements of the data	CIHI
Physical access control	The use of physical mechanisms to provide access control. Example: Keeping a computer in a locked room.	ISO/IEC 2382-08
Piggyback entry	Unauthorized access to a data processing system via an authorized user's legitimate connection	ISO/IEC 2382-08
Plaintext	Data, the semantic content of which is available without using cryptographic techniques [ISO 7498-2 m]	ISO/IEC 2382-08
Policy	A set of rules that specifies the procedures and mechanisms required to maintain the security of a system, and the security objects and security subject under the purview of the policy	HL7
Principal	Generally the party involved in communications and co-operations like user, application, system, etc. In the present scope: system or application	HL7
Privacy	Freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual	ISO/IEC 2382-08
Privacy protection	The measures taken to ensure privacy. NOTE: the measure include data protection and limitations on the gathering, combining and processing of data on individuals	ISO/IEC 2382-08
Private key	A key that is intended for decryption for the exclusive use by its owner	ISO/IEC 2382-08
Procedural security	Administrative measures for computer security. NOTE: those measures may be operational and accountability procedures, procedures of investigating breaches in security, and reviewing audit trails	ISO/IEC 2382-08
Protection profile	A reusable and complete combination of security objectives, functional and assurance requirements with associated rationals	CEN
Public key	A key that is intended for use by any entity for encrypted communication with the owner of the corresponding private key	ISO/IEC 2382-08
Public-key cryptography	Cryptography in which a public key and a corresponding private key are used for encryption and decryption.	ISO/IEC 2382-08

	NOTE: if a public key is used for encryption, the corresponding private key must be used for decryption, and vice versa.	
Read access	An access right that gives permission to read data	ISO/IEC 2382-08
Recovery	The restoration of an information system back to an error-free and secure state from which normal operation can resume	CEN
Release	The authorized disclosure of data or information to an individual or third party	COACH
Removal	The process of changing the location of an asset	COACH
Replay	The process of sending a previously sent message as a method of perpetrating a fraud	ASTM
Repudiation	The denial by one of the entities involved in a communication of having participated in all or part of the communication	ISO/IEC 2382-08
Residual data	Data left in a data medium after deletion of a file or a portion of a file. NOTE: residual data remain recoverable until sanitizing of the data medium has taken place.	ISO/IEC 2382-08
Retention	The process of holding data or information in secure or intact manner	COACH
Risk	The probability that a particular threat will exploit a particular vulnerability of a data processing system	ISO/IEC 2382-08
Risk acceptance	A managerial decision to accept a certain degree of risk, usually for technical or cost reasons	ISO/IEC 2382-08
Risk analysis	A systematic method of identifying the assets of a data processing system, the threats to those assets, and the vulnerability of the system to those threats	ISO/IEC 2382-08
Risk assessment	The systematic method of identifying the assets of a data processing system, the threats to those assets, and the vulnerability of the system to those threats	ISO/IEC 2382-08
Safeguards	Actions or measures taken to offset a particular security concern or threat	COACH
Sanitizing	Erasing or overwriting all data on a magnetic or other data medium, so that the data cannot be recovered	ISO/IEC 2382-08
<to>scavage	To search, without authorization, through residual data to acquire sensitive information	ISO/IEC 2382-08
Sector alignment	A technique for copy protection that determines whether a diskette is an unauthorized copy by checking whether sectors are positioned properly from track to track	ISO/IEC 2382-08
Secret key	A key that is intended for use by a limited number of correspondents for encryption and decryption	ISO/IEC 2382-08
Secure area	An area where health data is processed and/stored, or an area housing utilities or service facilities supporting health information equipment	COACH
Security	The combination of availability, confidentiality and integrity	CEN
Security association	The relationship between two entities which allows the protection of information communicated between the entities(<i>This relationship includes a shared symmetric key and security attributes describing the relationship. The security association is used to negotiate the characteristics of these protection mechanisms themselves</i>)	ASTM
Security audit	An independent review and examination of data processing system records and activities to test for adequacy of system controls, to ensure compliance with established security policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, security policy, and procedures	ISO/IEC 2382-08

Security breach	The unauthorized disclosure, destruction, modification or withholding of information	CEN
Security category	A non-hierarchical grouping of sensitive information used to control access to data more finely than with hierarchical security classification alone	ISO/IEC 2382-08
Security classification	The determination of which specific degree of protection against disclosure the information requires, together with a designation of that degree of protection. Examples: "Top secret", "secret", "confidential".	ISO/IEC 2382-08
Security clearance	Permission granted to an individual to access information at or below a particular security level	ISO/IEC 2382-08
Security filter	A trusted computer system that enforces a security policy on the data that pass through the system	ISO/IEC 2382-08
Security level	The combination of a hierarchical security classification and a set of security categories that represents the sensitivity of an object or the security clearance of a subject	ISO/IEC 2382-08
Security objective	A statement of intent to counter a given threat or enforce a given organizational security policy	CEN
Security policy	A plan or course of action adopted for providing computer security	ISO/IEC 2382-08
Security target	The statement of security requirements and functional specifications to be used as baseline for an evaluation	CEN
Sensitive information	Information that, as determined by a competent authority, must be protected because its disclosure, modification, destruction, or loss will cause perceivable damage to someone or something	ISO/IEC 2382-08
Sensitivity	A measure of importance assigned to information by the information owner to denote its need for protection	ISO/IEC 2382-08
Separation of duties	Dividing responsibility for sensitive information so that no individual acting alone can compromise the security of the data processing system	ISO/IEC 2382-08
Session	A logical relationship between two network endpoints that supports a user or network application	ASTM
Shell site	A alternative facility with at least the equipment necessary to support the installation and operation of a data processing system in the event of a disaster	ISO/IEC 2382-08
Single-level device	A functional unit that can only process data of a single security level at a particular time	ISO/IEC 2382-08
Software	Computer programs, procedures, and associated documentation and data pertaining to the operation of a computer system	COACH
Software piracy	The unauthorized use, copying, or distribution of software products. NOTE: this is an improved version of the definition in ISO/IEC 2382-1:1993	ISO/IEC 2382-08
Special privilege	Any feature or facility of a multi-user system that enables a user to override system or application controls	NHS
Spiral track	A track with a spiral shape written on a diskette, as part of a method of copy protection	ISO/IEC 2382-08
<to> spoof	To take action intended to deceive a user or a resource	ISO/IEC 2382-08
Standard	Documented agreements containing technical specifications or other precise criteria to be used consistently as rules, guidelines, or definitions of characteristics to ensure that materials, products, processes, and services are fit for their purposes (ISO 1996)	ISO/IEC 2382-08
Storage	The process of placing data or information in a location (e.g.,	COACH

	computer memory, storage device, secure area) for later use or disposal	
Strong authentication	Authentication by means of cryptographically derived credentials	CEN
Subject (in computer security)	An active entity that can access objects. Example: a process that involves execution of a program. NOTE: a subject may cause information to flow among objects or may change the state of the data processing system.	ISO/IEC 2382-08
Subnetwork	A network segment usually with its own address	ASTM
Substitution	Encryption that replaces bit strings or character strings with other bit strings or character strings. NOTE: the resulting ciphertext is called substitution cipher	ISO/IEC 2382-08
Supersector	An oversized sector written on a diskette, as part of a method of copy protection	ISO/IEC 2382-08
Symmetric cryptography	Cryptography in which the same key is used for encryption and decryption	ISO/IEC 2382-08
Symmetric encryption	Encryption using a single key to encrypt and decrypt which both the sender and receiver hold privately	ASTM
System integrity	The quality of a data processing system fulfilling its operational purpose while both preventing unauthorized users from making modifications to or use of resources and preventing authorized users from making improper modifications to or improper use of resources	ISO/IEC 2382-08
<to>tailgate	To gain unauthorized physical access by following an authorized person through a controlled door	ISO/IEC 2382-08
Threat	A potential violation of computer security	ISO/IEC 2382-08
Threat analysis	An examination of actions and events that might adversely affect a data processing system	ISO/IEC 2382-08
Threat assessment	An evaluation of the nature, likelihood and consequence of acts or events that could place sensitive data and assets at risk	COACH
Ticket (in computer security)	A representation of one or more access rights that a possessor has to an object. NOTE: the ticket represents an access permission	ISO/IEC 2382-08
Time bomb	A logic bomb to be activated at a predetermined time	ISO/IEC 2382-08
Top level security objective	A generalized statement of intended security goals relating to the availability, confidentiality and integrity of health care information	CEN
Traffic analysis	The inference of information from observation of traffic flow. Example: analysis of the presence, absence, amount, direction, and frequency of traffic	ISO/IEC 2382-08
Traffic padding	A countermeasure that generates spurious data in transmission media to make traffic analysis or decryption more difficult	ISO/IEC 2382-08
Transposition	Encryption that rearranges bits or characters according to some scheme. NOTE: the resulting ciphertext is called transposition cipher.	ISO/IEC 2382-08
Trapdoor	A hidden software or hardware mechanism, usually created for testing and troubleshooting, that may be used to circumvent computer security	ISO/IEC 2382-08
Trojan horse	An apparently harmless program containing malicious logic that allows the unauthorized collections, falsification, or destruction of data	ISO/IEC 2382-08
Trusted computer system	A data processing system that provides sufficient computer security to allow for concurrent access to data by users with different access rights and to data with different security classification and security categories	ISO/IEC 2382-08

Trusted third party	A security authority or its agent, trusted by other principal with respect to security-related activities	HL7
User	One who uses the services of a computer system	COACH
User ID	A character string or pattern that is used by a data processing system to identify a user	ISO/IEC 2382-08
User identification	A character string or pattern that is used by a data processing system to identify a user	ISO/IEC 2382-08
User profile (1)	A description of a user, typically used for access control. NOTE: a user profile may include data such as user ID, user name, password, access rights, and other attributes.	ISO/IEC 2382-08
User profile (2)	A pattern of a user's activity that can be used to detect changes in the activity	ISO/IEC 2382-08
Vaccine program	A program designed to detect viruses and possibly to suggest or take corrective action	ISO/IEC 2382-08
Verification	Comparing an activity, a process or a product with the corresponding requirements or specifications. Examples: comparing a specification with a security policy model or comparing object code with source code.	ISO/IEC 2382-08
Virtual private network	A network using public data network or the Internet as a carrier that acts as if a dedicated point to point network (cryptography is normally used to protect data)	ASTM
Virus	A program that propagates itself by modifying other programs to include a possibly changed copy of itself and that is executed when the infected program is invoked. NOTE: a virus often causes damage or annoyance and may be triggered by some event such as the occurrence of a predetermined date.	ISO/IEC 2382-08
Virus signature	A unique bit string that is common to each copy of a particular virus and that may be used by a scanning program to detect the presence of the virus	ISO/IEC 2382-08
Vulnerability	A weakness or flaw in a data processing system. NOTE: if a vulnerability corresponds to a threat, a risk exists	ISO/IEC 2382-08
WAN	Acronym for Wide Area Network	COACH
Weak bit	A bit intentionally written on a diskette with a weak magnetic field strength that may be interpreted as zero or one and that is written as part of a method of copy protection	ISO/IEC 2382-08
Wide track	A set of two or more adjacent tracks written on a diskette with the same data, as part of a method of copy protection	ISO/IEC 2382-08
Wiretapping	Surreptitious access to a line to obtain, modify, or insert data	ISO/IEC 2382-08
Worm	A self-contained program that can propagate itself through data processing systems or networks. NOTE: worms are often designed to use up available resources such as storage space or processing time	ISO/IEC 2382-08
Write access	An access right that gives permission to write data. NOTE: write access may grant permission to append, modify, delete, or create data.	ISO/IEC 2382-08