

---

Department: UW Medicine Information Technology Services

Policy Number: SEC-REF UW Medicine Security Program Glossary of Terms

Effective Date:

Review Date:

---

Term	Definition
<b>Access</b>	Access is the ability to do something with a computer resource (e.g., use, change, or view)
<b>Access Control</b>	Access Control is physical, procedural and/or electronic mechanism, which ensures that only those who are authorized to view, update and/or delete data can access that data, and includes the prevention of use of a resource in an unauthorized manner.
<b>Access Management</b>	Policies, systems, and processes that determine how access decisions will be made (e.g., role-based), assign access profiles to users and other identities, and store access information in local or central repositories for use by information systems. Included are processes to maintain correct access profiles as the roles or affiliations of individuals change over time.
<b>Aggregate Data</b>	<p>Aggregate Data is a <i>collection-oriented</i> dataset (report or query results) where information is composed with the elements of data from multiple patients formed from one or several separate source systems.</p> <p>The health information may or may not be individually identifiable.</p> <p>Aggregate data may be system generated or constructed by a user collecting information and adding it to data saved from other events.</p> <p>The dataset may come from one application or system or it may be derived from multiple applications and diverse systems.</p> <p>Often an effective method for presenting and distributing information for QA, monitoring outcomes, business reviews, and research.</p>
<b>Anti-virus Controls</b>	All systems connected to the UW Medicine network are required to have virus protection. Information Technology Services will maintain and update a list of approved software for virus protection.
<b>Asymmetric Cryptosystem</b>	A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).
<b>Audit</b>	An audit is an evaluation of an organization, department, system, process or application done to assess compliance with applicable regulations, policies, standards, or procedures.
<b>Authentication</b>	Authentication is a systematic method for establishing proof of identity.
<b>Authorization</b>	Authorization is the process of giving someone permission to do or have something; a system administrator defines for the system which users are allowed access to the system and what privileges are assigned. The system could be an operating system, database, or an application.
<b>Authorized Data Users</b>	Person's who based on role/function/responsibility have access to protected health information.

<b>Authorized Software</b>	Software that is authorized for use by the designated System Owner or Department Manager.
<b>Availability</b>	Ensuring that authorized users have access to information and associated assets when required.
<b>Breach</b>	A bypass of controls to gain unauthorized access to UW Medicine information assets.
<b>Business Associate</b>	A person or entity, other than a member of the UW Medicine workforce, who performs certain functions, activities or services for or on behalf of UW Medicine, involving the use and/or disclosure of protected health information.
<b>Business Contingency Plan</b>	A plan for identifying, evaluating, and implementing actions to mitigate and prevent emergency interruptions.
<b>Business Impact Analysis</b>	Identifies, prioritizes, and documents critical business processes including specific recovery objectives that feed the business contingency strategy and plan.
<b>Class (Job class)</b>	Individuals within a group who have the same role and responsibilities (e.g., Nurse practitioners, physicians) a “need-to-know” permission access applications.
<b>Common Criteria for Information Security Evaluation</b>	Common Criteria for Information Security Evaluation is a comprehensive specification (aligned with the ISO IS 15408) that first defines the targeted environment and then specifies the security requirements necessary to counter threats inherent in that environment.
<b>Communication security</b>	Information transmitted outside the UW Medicine requires protection. Methods employed will depend upon information sensitivity, technical risks and threats, external regulations and available communication security controls.
<b>Confidentiality</b>	Ensuring that information is accessible only to those authorized to have access.
<b>Confidential information</b>	Confidential information is very sensitive in nature and requires careful controls and protection. Unauthorized disclosure of confidential information could seriously and adversely impact UW Medicine or interests of patients, other individuals, and organizations associated with UW Medicine. Confidential information includes, but is not limited to, personally identifiable information, protected health information, workforce records, student records, social security numbers, legally protected University records, research data, passwords, intellectual property.
<b>Controls</b>	The policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.
<b>Cookie</b>	A cookie is small text file that is placed on a user’s hard drive by the Web site that the user is visiting. This file records preferences and other data about your visit to that particular site. This is most evident when a user returns to a site and is greeted by name. Cookies are often used for long-term data collection. Short-term cookies might be used for things like authentication in “single sign-on” services.
<b>Cost-effective</b>	Cost-effective is to deliver desired results in beneficial financial terms.
<b>Covered Entity</b>	A “Covered Entity” includes any of the following types of health care business organizations or individuals which transmit or maintain protected health information in electronic or other form or medium including:

	<input type="checkbox"/> Health care provider (e.g., hospital or physician), <input type="checkbox"/> Health care plan (e.g., managed care program), <input type="checkbox"/> Health care clearinghouse (e.g., third-party billing center)
<b>Critical Servers</b>	Critical Servers: Within UW Medicine these are devices needed to support patient care, financial services or contain proprietary information that has value in and of itself.
<b>Critical Systems and Services</b>	Systems and services that have been identified as critical due to the fact that they directly support or are necessary for effective patient care.
<b>Data Custodians</b>	Data Custodians: Individuals who have been officially designated as accountable for protecting the confidentiality of specific data that is transmitted, used, and stored on a system or systems within a department, college, school, or administrative unit
<b>Data Integrity</b>	The property that data has not been altered or destroyed in an unauthorized manner.
<b>Decryption</b>	Decryption is the process of turning unreadable cipher text into readable text.
<b>Department Administrator/Manager</b>	Accountable for the management of their workforce that make use of UW Medicine information systems, databases, or applications.
<b>Detective Controls</b>	Controls are designed to detect errors and irregularities which have already occurred and to assure their prompt correction. Detective controls supply the means with which to correct data errors, modify controls or recover missing assets.
<b>Digital Hash</b>	The string of bits that is the output of an algorithm for computing a condensed representation of a message or a data file.
<b>Digital Signature</b>	A method of signing an electronic message that identifies and authenticates a particular person as the source of the electronic message.
<b>Direct Threats</b>	Direct Threats occur when an individual attempts to gain unauthorized access to, or get possession of your assets. The direct threat often receives the most attention because it is easiest to identify. Within health care, direct threats may take the form of hackers attempting to break into your computers, the theft of a personal computer, or entering a secure area. Keep in mind that your assets don't have to be tangible to be real; the value of your reputation and your information may be higher than the value of your equipment.
<b>Disaster Recovery Planning</b>	All data centers and computerized systems critical to the UW Medicine must have written and operationally tested disaster recovery plans. Data custodians in conjunction with information custodians will prioritize the recovery of applications and associated data.
<b>Disclosure</b>	Release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information for any purpose other than treatment.
<b>Domain</b>	A group of systems that are under the control of the same security authority.
<b>Email Client</b>	Software used by a user to interact with their mailbox server in order to read and send email, or work with email folders. Examples include Pine, WebPine, Outlook Express, Outlook, Eudora, etc. Which are also called Mail User Agents (MUA).

<b>Email Relay</b>	An email server that receives email from a variety of sources and that routes the email towards its final destination. A pure email relay does not host any Inboxes or user mail folders. Instead, it functions as a mail router on the network. a.k.a. Mail Transfer Agent (MTA)
<b>Encryption</b>	Encryption is the process of turning readable text into unreadable cipher text.
<b>ePHI</b>	Protected Health Information transmitted by electronic media or maintained in electronic media
<b>External Audit</b>	An audit performed by an independent group or individual that comes from outside the organization being audited. External audits are often requested by an organization as a means to verify internal audit finding, but they may also be externally imposed as part of a regulatory investigation.
<b>Firewalls</b>	Firewalls: Policy-based filtering systems (composed of both hardware and software) that control and restrict the flow of data between networked computer systems. Firewalls establish a physical or logical perimeter where selected types of network traffic.
	Integrated OS firewalls, bundled with the OS (e.g. Windows, Linux)
	Dedicated firewalls protecting labs or server sanctuaries
	Dedicated firewalls protecting individual hosts
	Logical firewalls protecting non-co-located systems
<b>Forensics (computer)</b>	Forensics (computer): The discipline of dissecting computer storage media, log analysis, and general systems and data examination to find evidence of computer crime or other violations.
<b>Guideline</b>	A document that recommends a particular approach, course of action, or configuration based on generally accepted best practices. Compliance with guidelines is not compulsory but is expected whenever it is feasible.
<b>Health Care Operations</b>	UW Medicine healthcare operations are those business functions required for managing and delivering health and medical services. These include all business processes relating to the following:
	<u>Business Focused Activities</u>
	<input type="checkbox"/> General administrative functions (e.g., limited fundraising and marketing, HIPAA compliance),
	<input type="checkbox"/> Business planning and development (e.g., cost management analyses, planning-related analyses, formulary development, payment methods and coverage policies),
	<input type="checkbox"/> Disclosure of protected health information for legal and regulatory purposes,
	<input type="checkbox"/> Internal grievance resolution,
	<input type="checkbox"/> Customer service, provided health information is not disclosed,
	<input type="checkbox"/> Accreditation, certification, licensing or credentialing activities,
	<input type="checkbox"/> Health insurance contracting (e.g., underwriting, premium rating, reinsurance of risk relating to claims),
	<input type="checkbox"/> Medical review, legal services and auditing functions (e.g., fraud and abuse detection and compliance programs).

	<p><u>Clinically-Focused Activities</u></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Quality assessment including outcomes evaluation,</li> <li><input type="checkbox"/> Clinical guidelines and clinical protocol development,</li> <li><input type="checkbox"/> Case management and care coordination,</li> <li><input type="checkbox"/> Patient contact regarding treatment alternatives,</li> <li><input type="checkbox"/> Performance evaluation for healthcare professionals, providers, and practitioners,</li> <li><input type="checkbox"/> Training programs for students, practitioners and non-healthcare professionals.</li> </ul>
<b>High Risk</b>	The unauthorized disclosure of, improper modification or destruction of, or disruption of access to information could be expected to have a severe adverse effect on operations, assets or public image.
<b>Hospital Emergency Incident Command System (HEICS)</b>	The External Disaster Plan for the Medical Centers.
<b>Hybrid Entity</b>	A single legal entity that is a covered entity and whose covered functions are not its primary functions. The University of Washington (UW) has both health care components and Non- health care components. The health care components and other components
<b>Hyper Text Transfer Protocol (HTTP)</b>	A protocol primarily used for communications between a web browser and a web server.
<b>Identification</b>	Process or mechanism by which a user, computer, or application asserts the identity (e.g., user ID, PIN, account name) they intend to use for access to information or an information system.
<b>Identity Management</b>	Policies, systems, and processes that control how individuals are identity proofed, registered, and assigned a digital identity. Included are processes to aggregate appropriate personal data about individuals, including their affiliations within the organization, and to track changes to this information over time.
<b>Identity Proofing</b>	A process that provides some of level of assurance that a person is who they claim to be, usually through examination of government issued documents and photo IDs. Identity proofing is a prerequisite for the user registration process.
<b>Incident Response</b>	Incident Response is the ability to respond appropriately and completely to any incidents, situational compromises, or threats from any source.
<b>Indirect Threats</b>	Indirect Threats are random situations where your organization is not specifically an intended target. "Catching" a computer virus is likely the result of an indirect threat.
<b>Individual</b>	Person who is the subject of protected health information.
<b>Information Security Incident</b>	An event kicked off by the report of a UW Medicine Security Policy violation or a violation of a legal standard, such as, a State or Federal Law violation.
<b>Information System(s)</b>	A logical and reasonable delineation of computing resources that may be based upon software, hardware, and/or data to allow for the management, administration, and protection of these computing resources.
<b>Integrity</b>	Safeguarding the accuracy, completeness, and control of information and processing methods.

<b>Internal Audit</b>	An audit performed by a group or individual that comes from inside the organization being audited. The goal of internal audits is to identify gaps for targeted performance improvements.
<b>Internet Mail Access Protocol (IMAP)</b>	A protocol used by email client software to download email messages and attachments from a mailbox server.
<b>Intrusion</b>	An intruder, individual(s) who are not legitimate user(s) or not authorized user(s), has attempted to gain or has gained unauthorized access to a system.
<b>Intrusion Detection System</b>	Intrusion Detection is a security management system that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attack from outside the organization) and misuse (attacks from within the organization).
<b>IT Risk Management</b>	IT Risk Management is a comprehensive methodology that strives to balance risks against benefits in a pre-defined environment.
<b>Licensed software</b>	Software that the University of Washington has been granted permission from the owner to use under a written license agreement or contract.
<b>Limited Adverse Effect</b>	(i) cause degradation in mission capability to an extent and duration that UW Medicine is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to UW Medicine assets; (iii) result in minor financial loss; or (iv) result in no harm to individuals.
<b>Malicious Software</b>	Malicious software includes, but is not limited to: computer viruses, network worms, Trojan horses and logic bombs.
<b>Mail Application Programming Interface (MAPI)</b>	A protocol used by some email clients (e.g., Microsoft Outlook) to communicate with some email servers (e.g., Microsoft Exchange). MAPI operates over RPC and there is an option to encrypt the session.
<b>Mailbox Server</b>	An email server that is responsible for storing and retrieving a user's email in their Inbox or other mail folders.
<b>Memorandum of Understanding (MOU)</b>	For the purposes of this policy, a MOU is a written agreement between UW Medicine and an external party formally documenting the relationship and defining the roles, responsibilities, expectations, agreed terms, and conditions in relation to the other or others with respect to access and use of UW Medicine patient identifiable information.
<b>Minimum Necessary</b>	"Minimum necessary" protected health information is defined as that "limited" health information required to perform a business activity or achieve an authorized requestor's specified purpose. Minimum necessary is based on the "need to know" principle.
<b>"Need-to-Know" Principle</b>	Limiting access to information to that required for the user's job function or role and responsibilities.
<b>Networked System</b>	A Networked System is a computer system or PC interconnected with other computer systems using wired or wireless network technologies.
<b>Non-repudiation</b>	Non-repudiation is a mutually agreed process, secured evidence, or other method of operation, which provides for proof of receipt or protection from denial of an electronic transaction or other activity.
<b>Notice of Privacy Practices</b>	UW Medicine entities post and distribute a statement of privacy practices describing notified of the types of uses and disclosures of protected health information (PHI) and have the right to be notified of individual patient rights and UW Medicine's legal duties with respect to that information. When patients present for care, each entity within the UW Medicine

	Covered Entity collects a signed acknowledgement, that the individual or personal representative/surrogate decision maker has been provided the UW Medicine Notice of Privacy Practices (Notice).
<b>Organized Healthcare Arrangement</b>	<input type="checkbox"/> A clinically-integrated care setting in which individuals typically receive healthcare from more than one health care provider; OR <input type="checkbox"/> An organized health care system in which more than one covered entity participates, and which the covered entities are publicly known to jointly work together and one of the following activities is performed: <ul style="list-style-type: none"> <li><input type="checkbox"/> Utilization review,</li> <li><input type="checkbox"/> Quality assessment and improvement,</li> <li><input type="checkbox"/> Payment activities.</li> </ul>
<b>Ownership</b>	Ownership: The term that signifies decision-making authority and accountability for a given span of control.
<b>Patient</b>	A UW Medicine patient is any individual who receives health services through any one of UW Medicine's health care facilities. Health services include any direct health care treatment, health services planning and coordination, and includes participants and/or subjects in clinical research activities.
<b>Patient Identifiable Information'</b>	Specific to Healthcare and 'patient identifiable information' it includes any of the following information related to patients, patient's relatives, employers, or household members: name, address (including street address, city, county, zip code, and equivalent geocodes), names of relatives, names of employers, date of birth, telephone numbers, fax numbers, electronic mail addresses, Social Security number, medical record number, health plan beneficiary number, account numbers, certificate/license number, any vehicle or other device serial number, Web Universal Resource Locator (URL), personal Internet Protocol (IP) address number, bio-metric data (finger or voice prints), photographic images, and any other unique identifying number, characteristic or code that UW member employee has reason to believe may be available to the anticipated recipient of information.
<b>PDA</b>	Short for <u>p</u> ersonal <u>d</u> igital <u>a</u> ssistant, a handheld device that may combine computing, telephone/fax, internet and networking features. A PDA can function as a cellular phone, fax sender, web browser and personal organizer.
<b>Personally Identifiable Information</b>	Personally Identifiable Information is specific data, elements of non-specific aggregate data, or other information which is tied to, or which otherwise identifies, an individual or provides information about an individual in a way that is reasonably likely to enable identification of a person as an individual and make personal information about them known.
<b>Policy</b>	A document that specifies general requirements or rules that must be followed by all parties to which they apply. These requirements guide decision making throughout an organization and help it achieve security, compliance, and other objectives.
<b>Post Office Protocol (POP)</b>	A protocol used by email client software to download email messages and attachments from a mailbox server.
<b>Pretty Good Privacy (PGP)</b>	An alternate mechanism for digitally signing and/or encrypting email based on public key cryptography. There are both open source and

	commercial versions available.
<b>Principle of Least Privilege</b>	Principle of Least Privilege: Access privileges for any user should be limited to only what they need to have (nothing in addition) to be able to complete their assigned duties or functions.
<b>Principle of Separation of Duties</b>	Principle of Separation of Duties: Whenever practical, no one person should be responsible for completing or controlling a task, or set of tasks, from beginning to end when it involves the potential for fraud, abuse or other harm.
<b>Privacy</b>	Privacy: An individual right to be left alone; to withdraw from the influences of his or her environment; to be secluded, not annoyed, and not intruded upon; to be protected against the misuse or abuse of something legally owned by an individual.
<b>Procedure</b>	A document that describes detailed steps for completing a particular action in a consistent and repeatable way in order to comply with a policy or standard
<b>Proprietary Information</b>	Proprietary information is any information or material (including, but not restricted to, ideas, concepts, proposals, inventions, instruments, samples, cost estimates, data, and computer programs) that UW Medicine has exclusively developed.
<b>Proprietary Encryption</b>	An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.
<b>Protected Health Information (PHI)</b>	Individually identifiable health information maintained in permanent health records and/or other clinical documentation in either paper-based or electronic format.
<b>Pulverized</b>	Pulverized Means reduced, as by crushing, beating, or grinding to very small particles that cannot be reconstructed or used in any combination to reconstruct the original.
<b>Recovery Point Objective (RPO)</b>	Specified time period for which data needs to be recovered in order that our business may re-launch operations after a disaster occurs.
<b>Recovery Time Objective (RTO)</b>	Specified amount of time you have to bring a system back online after a disaster before it significantly impacts business operations.
<b>Registration Authority</b>	An administrative group responsible for identity proofing individuals, entering them into an identity management system, and maintaining their data over time.
<b>Remote Procedure Call (RPC)</b>	A programmatic method for software running on one computer to communicate with software running on the same or another computer.
<b>Repudiation</b>	Denial by one of the individuals or entities involved in a communication of having participated in all or part of the communication.
<b>Restricted Information</b>	Restricted Information is business data that is intended strictly for use by designated UW Medicine employees and agents. This classification applies to data less sensitive than CONFIDENTIAL information. Dissemination of this data shall only be made to UW Medicine workforce with an established need-to-know.
<b>Risk Assessment</b>	System review which includes: (1) evaluation of risk to confidentiality, integrity, and availability; (2) threat and vulnerability identification and analysis; and (3) results documentation.
<b>Risk Management</b>	Risk Management is a comprehensive methodology that strives to balance risks against benefits in a pre-defined environment

<b>Role-based Access</b>	Providing access to protected health information based on user's job function (role and responsibilities). UW Medicine guidelines establish that user's may access health information assets only on a need to know basis and must be approved and verified as Authorized Data Users. Examples include: physician, resident, nurse, physician assistant, and others.
<b>Safeguards</b>	Administrative, technical, and physical controls which are implemented and maintained for the purpose of protecting information and information systems.
<b>Secure Area</b>	An area designated area by System Owners and UW Medicine departments that requires an additional level of protection to minimize unauthorized access, damage, and interference to information and information systems,
<b>Secure Multipart Internet Mail Extension (SMIME)</b>	An Internet standard mechanism for digitally signing and/or encrypting email based on public key cryptography. SMIME is built into many email clients (e.g., Outlook, Outlook Express).
<b>Secure Sockets Layer (SSL)</b>	An encryption protocol that establishes a secure tunnel between two computers.
<b>Security</b>	Security: An attribute of information systems which includes specific policy-based mechanisms and assurances for protecting the confidentiality and integrity of information, the availability and functionality of critical services and the privacy of individuals.
<b>Security Controls</b>	Information security is achieved by implementing a suitable set of controls, which include policies, practices, procedures, structures and functions. These controls need to be established and serve to ensure that specific information security objectives of UW Medicine are met. Controls for information security are established for Physical and Environmental, Hardware and Software Maintenance, System and Information Integrity, Media Protection, Identification and Authentication, Logical Access Control, Accountability (including Audit Trails), System and Communications Protection.
<b>Server Sanctuaries</b>	Server Sanctuaries (a.k.a. Safe Sanctuaries): Within UW Medicine, these are locations within computing facilities where clusters of sensitive or critical servers can be co-located and around which suitable physical and logical security measures can be implemented.
<b>Sensitive Servers</b>	Sensitive Servers: Within UW Medicine these are devices that contain personally identifiable data or other sensitive information.
<b>Serious Adverse Effect</b>	(i) cause a significant degradation in mission capability to an extent and duration that UW Medicine is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to UW Medicine.
<b>Server System</b>	A Server System is a type of Networked System that serves data or other resources to users or other systems across a network. Examples include file servers, web servers, and database servers.
<b>Severe Adverse Effect</b>	(i) cause a severe degradation in or loss of mission capability to an extent and duration that UW Medicine is not able to perform one or more of its primary functions; (ii) result in major damage to UW Medicine assets; (iii) result in major financial loss
<b>Simple Mail Transfer Protocol (SMTP)</b>	A protocol used by email clients to send messages to a specified mail relay as the first step towards delivery of a message to its intended recipient. SMTP is also used to send email from relay to relay on its way

	to its final destination.
<b>SIT</b>	UW Medicine Information Technology Services' Security Infrastructure Team
<b>Smart Phones</b>	Smart phones have strong processors and flexible Operating Systems, which provide 24/7 internet connectivity. Smart phones features may include: email, calendar, contacts, task lists, Microsoft Office documents, reading PDFs, Media Player, instant messaging.
<b>Standard</b>	A document that specifies specific requirements or rules that must be followed by all parties to which they apply. Standards are generally more specific than policies and often target particular kinds of systems, technologies, or business processes. Standards provide a reference point for security evaluations and risk assessments.
<b>STARTTLS</b>	STARTTLS is an SMTP command used by a sending system to request that the receiving system use TLS encryption (essentially SSL) for the current mail transfer session. Depending on the receiving system's capability and configuration, it may or may not honor the request. If a SMTP system is configured to always use TLS and another SMTP system does not comply, the mail transfer session will be terminated.
<b>Symmetric Cryptosystem</b>	A method of encryption in which the same key is used for both encryption and decryption of the data (e.g. shared secret)
<b>System Operators</b>	System Operators: Individuals within UW Medicine who are accountable for the operational decisions about the use and management of a computing system. (See also, 'System Owners').
<b>System Owners</b>	System Owners are individuals within the UW Medicine community who are accountable for the management and use of one or more electronic information systems, electronic databases, or electronic applications that are associated with UW Medicine. System Owners.
<b>Threat</b>	A threat is a type of harm that could significantly impact system or data confidentiality, integrity, and/or availability.
<b>Threat action</b>	Methods by which an attack used by an insider or outsider might be executed to accomplish a compromise a computer network or host (computer).
<b>Threat source</b>	Both (1) intent and method targeted at the intentional exploitation of vulnerability or (2) a situation and method that may accidentally trigger vulnerability Examples: Terminated employees, Hackers.
<b>TPO</b>	<u>T</u> reatment, <u>P</u> ayment or Health Care <u>O</u> perations – Term used throughout HIPAA Privacy regulations.
<b>Use</b>	The sharing, employment, application, utilization, examination, or analysis of individually identifiable health information maintained by an entity.
<b>Users</b>	Any individual using a computer connected to UW Medicine networks or those who has been granted privileges and access to UW Medicine computing and network services, applications, resources, and information.
<b>User authentication</b>	User authentication is the provision of assurance of claimed identity of an individual (entity).
<b>UW-managed network</b>	UW-managed network: a network operated by the UW where all the components and network-attached computers are operated in accordance with UW-approved systems management practices to ensure secure, reliable, and policy-compliant operation.

	A message that travels over a UW-managed network from sender to recipient is considered to use a “private” network and hence does not require additional access control methods or other security measures for most applications and use.
<b>UW Medicine</b>	UW Medicine includes the following entities: University of Washington Medical Center and Clinics; Harborview Medical Center and Clinics; UW Medicine Neighborhood Clinics (University of Washington Physicians Network); UW Physicians Sports Medicine Clinic;
<b>UW Medicine enterprise systems</b>	The information systems distributed and maintained by IT Services for use across UW Medicine. (Examples: EPIC, MINDscape, ORCA, and PEPP.)
<b>UW-owned network</b>	<p>UW-owned network: a network where all network components, including active elements such as routers and switches, and transmission media, and all network-attached computers are owned and operated by the UW or subunits of the UW. A message that travels over networks that are UW-owned but not “UW-managed” should in general be considered to be on an open network and hence require additional security measures to be considered secure.</p> <p>A message that travels over a non-UW-owned network is assumed to use an open network (e.g. public Internet wire) and therefore requires additional protections, unless all of the non-UW-owned networks are covered under business arrangements that control access sufficiently so that they are considered to be private.</p>
<b>Virtual Private Network (VPN)</b>	A virtual private network (VPN) is a way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network where the session is protected by authentication.
<b>Vulnerability</b>	A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.
<b>Workforce</b>	Faculty, employees, trainees, volunteers, and other persons who perform work for UW Medicine, and whose work conduct is under UW Medicine's direct control regardless of whether or not they are paid by UW Medicine.