

Updated: July 01, 2009

[Privacy/Security Glossary of Common Terms](#)

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)

A

Acceptable Risk: The level of risk management finds acceptable to a particular information asset. Acceptable risk is based on empirical data and supportive technical opinion that the overall risk is understood and that the controls placed on the asset or environment will lower the potential for its loss. Any remaining risk is recognized and accepted as an accountability issue.

Acceptable Use Policy (AUP): A set of rules and guidelines that specify in more or less detail the expectations in regard to appropriate use of systems or networks.

Access Control: The prevention of unauthorized use of information assets. It is the policy rules and deployment mechanisms, which control access to information systems, and physical access to premises.

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

Administrative Hearing: An oral proceeding before an administrative law judge in a contested case hearing.

Administrative Order: An order that has the same meaning as the definition in ORS 183.310(5)(a), where an "order" means any agency action expressed orally or in writing directed to a named person or named persons, other than employees, officers or members of an agency.

Administrative Safeguards: Administrative actions and policies and procedures, to manage the selection, development, implementation and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.

Administrative Tribunal: The entity authorized by state law to preside over an administrative proceeding, whether conducted by the director or administrator, or designated employee, of an Oregon state agency or before an administrative hearing officer in a contested case hearing pursuant to Oregon law, that may result in an Administrative Order (defined above).

Authentication: The act of verifying the identity of an individual, originator, terminal, or workstation, to determine that entity's right to access specific categories of information and a measure designed to protect against fraudulent transmission by verifying the validity of a transmission, message, station, or originator.

Authorization: Permission from an individual, or his or her personal representative giving the Department of Human Services (Department) authorization to obtain, release or use information about the individual from third parties for specified purposes or to disclose information to a third party specified by the individual.

Authorized Representative: A person who has authority under program rule to act on behalf of the individual in making an application for the program, reporting changes, or obtaining or using benefits.

Availability: Assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them and that the information it provides will be of acceptable integrity.

B

Business Associate: An individual or entity performing any activity or function on behalf of the Department involving the use or disclosure of protected health information (PHI) and is not a member of the Department's workforce.

- "Function or activity" includes but is not limited to: program administration, claims processing or administration, data analysis, utilization review, quality assurance, billing, legal, actuarial, accounting, consulting, data processing, management, administrative, accreditation, financial services, and similar services for which the Department may contract, if access to PHI is involved.
- Business associates do not include licensees or providers unless the licensee or provider also performs some "function or activity" on behalf of the Department.

[Back to top](#)

C

Client: An individual who requests or receives services from the Department. This includes but is not limited to: applicants for or recipients of public assistance; minors and adults receiving protective services; Oregon Health Plan members or enrollees; individuals who apply for or are admitted to a state training center or a state hospital or who are committed to the custody of the Department; children in the custody of the Department receiving services on a voluntary basis; and children committed to the custody of the Department.

Client Information: Personal information relating to a client that the Department may maintain in one or more locations and in various forms, reports, or documents, or stored or transmitted by electronic media.

Client Records: All personal information that DHS has collected, compiled, or created about DHS clients, which DHS may maintain in one or more locations and in various forms, reports, or documents, including information that is stored or transmitted by electronic media.

Client Services: The provision of assistance, care, treatment, training or support to a client by DHS.

Collect/Collection: The assembling of personal information through interviews, forms, reports, or other information sources.

Compliance: Adherence to those policies, procedures, guidelines, laws, regulations and contractual arrangements to which the business process is subject.

Confidentiality: The degree to which sensitive data, about both individuals and organizations, must be protected. Information is not made available or disclosed to unauthorized individuals, entities, or processes.

Confidential Information: Any client information (defined above) that DHS may have in its records or files on any DHS client that must be safeguarded pursuant to DHS policy. This includes, but is not limited to, "individually identifying information" (defined below).

Contract: A written agreement between the Department and a person or entity setting forth the rights and obligations of the parties including but not limited to contracts, licenses, agreements, interagency agreements, and intergovernmental agreements.

Cookies: Cookies register information about a visit to a Web site for future use by the server. A server may receive information of cookies of other sites as well, which create concern in terms of breach of privacy.

Correctional Institution: Any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by contract with the United States, a State, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. "Other persons held in lawful custody" include juvenile offenders, adjudicated delinquents; aliens detained awaiting deportation, witnesses, or others awaiting charges or trial.

Corrective Action: An action that a Department business associate must take to remedy a breach or violation of the business associate's obligations under the business associate contractual requirement, including but not limited to reasonable steps that must be taken to cure the breach or end the violation.

Covered Entity: Health plans, health care clearinghouses, and health care providers who transmit any health information in electronic form in connection with a transaction that is subject to federal Health Insurance Portability and Accountability Act (HIPAA) requirements, as those terms are defined and used in the HIPAA regulations, 45 CFR parts 160 and 164.

Cure Letter: A letter sent by one party to another, proposing or agreeing to actions that a party will take to correct legal errors or defects that have occurred under a contract between the parties or other legal requirement.

[Back to top](#)

D

Data Classification: The conscious decision to assign a level of sensitivity to data as it is being created, amended, enhanced, stored, or transmitted. The classification of the data then determines the extent to which the data needs to be controlled / secured and is indicative of its value in terms of information assets.

Decrypting: The process of reversing the encryption of a file or message to recover the original data in order to use or read it.

De-identified Data: Client information from which the Department or other entity has deleted, redacted, or blocked identifiers, so the remaining information cannot reasonable be used to identify an individual.

Department: The Department of Human Services (DHS).

Department Workforce: Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the Department, is under the direction and control of the Department, whether or not they are paid by the Department.

DHS: The Department of Human Services, also referred to as "the department."

Digital Signature: A mathematical computer program creates a digital signature. It is neither a hand-written signature nor a computer-produced picture of one. The signature is like a wax seal that requires a special stamp to produce it, and is attached to an email message or file. The digital signature may then verify the origin of the message or file.

Disclose: The release, transfer, relay, provision of access to, or conveying of client information to any individual or entity outside the Department.

Downloading: The act of retrieving files from a server on the network.

E

Employee: A public employee or officer for whom DHS is the appointing official.

Encryption: The process by which data is temporarily re-arranged into an unreadable or unintelligible form for confidentiality, transmission, or other security purposes.

EPHI: Electronic Protected Health Information (EPHI)

F

Facility: The physical premises and the interior and exterior of a building.

Facility Directory: A listing or reference document maintained by a health care provider, such as (but not limited to) a hospital, nursing home, or treatment center, of persons receiving care or treatment from that provider and containing information about each individual patient or resident receiving care or treatment.

File Server: A computer system that provides a way of sharing and working on files stored on the system among users with access to these files over a network.

FTP (File Transfer Protocol): A protocol that allows for the transfer of files between an FTP client and FTP server.

[Back to top](#)

H

Health Care: Care, services or supplies related to the health of an individual. Health care includes but is not limited to preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care and counseling services, assessment, or procedure with respect to the physical or mental condition, or functional status of an individual, or that affects the structure or function of the body and the sale or dispensing of a drug, device, equipment, or other prescribed item.

Health Care Operations: Any of the following activities of the Department to the extent that the activities are related to health care, Medicaid or any other health care related programs, services, or activities administered by the Department:

- Conducting quality assessment and improvement activities, including income evaluation and development of clinical guidelines.
- Population-based activities related to improving health or reducing health care costs, protocol development, case management and care coordination, contacting health care providers and patients with information about treatment alternatives; and related functions that do not include treatment.
- Reviewing the competence of qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students and trainees in areas of health care learn under supervision to practice or improve their skills, accreditation, certification, licensing, or credentialing activities.
- Underwriting, premium rating, and other activities relating to the creation, renewal, or replacement of a contract for Medicaid or health care related services.
- Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs, and disclosure to the Medicaid Fraud Unit pursuant to 43 CFR part 455.21.
- Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the Department, including administration, development or improvement of methods of payments or health care coverage.
- Business management and general administrative activities of the Department, including but not limited to the following:
 - Management activities relating to implementation of and compliance with the requirements of HIPAA;

- Customer service, including providing data analysis;
- Resolution of internal grievances, including administrative hearings and the resolution of disputes from patients or enrollees regarding the quality of care and eligibility for services.
- Creating de-identified data or a limited data set.

Health Oversight Agency: An agency or authority of the United States, a state, territory, political subdivision of a state or territory, or Indian tribe, or a person or entity acting under a grant of authority from or by contract with the public agency, including employees or agents of the public agency or its contractors or grantees that is authorized by law to oversee the health care system or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant. When performing these functions, the Department acts as a Health Oversight Agency for the purposes of these rules.

HIPAA: The Title II, Subtitle F of the Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d et seq, and the federal regulations adopted to implement the Act.

[Back to top](#)

I

Individual: The person who is the subject of information collected, used, or disclosed by the Department.

Individually Identifying Information: Any single item or compilation of information or data that indicates or reveals the identity of an individual, either specifically (such as the individual's name or social security number), or from which the individual's identity can reasonably be ascertained.

Information: Personal information relating to an individual, a participant, or a Department client.

Information Asset: Refers to any information in any form (e.g. written, verbal, oral or electronic) upon which the organization places a measurable value. This includes information created by DHS, gathered for DHS, or stored by DHS for external parties.

Information Owner/User: An (human) individual that makes use of computer systems and networks.

Information Security: Management and technology programs to protect the organization from unacceptable risks to the organization's information assets. The mechanisms and practices to protect confidential and sensitive information.

Information Security Office: Information Security Office (ISO) was established within DHS. This office manages the departments' Privacy and Security programs.

Information Systems: The computer systems and information sources used by an organization to support its day-to-day operations.

Inmate: A person incarcerated in or otherwise confined in a correctional institution. An individual is no longer an inmate when released on parole, probation, supervised release, or is otherwise no longer in custody.

Institutional Review Board (IRB): A specially constituted review body established or designated by an entity in accordance with 45 CFR part 46 to protect the welfare of human subjects recruited to participate in biomedical or behavioral research. The IRB must be registered with the Office for Human Research Protection.

Integrity: The property that data or information have not been altered or destroyed in an unauthorized manner.

L

Law Enforcement Official: An officer or employee of any agency or authority of the United States, a State, territory, political subdivision of a State or territory, or Indian tribe, who is empowered by law to:

- Investigate and conduct an official inquiry into a potential violation of law; or
- Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Licensee: A person or entity that applies for or receives a license, certificate, registration, or similar authority from the Department to perform or conduct a service, activity, or function.

Log In, Logging into a System: This is an action performed by an end-user, when he authenticates himself to a computer system.

[Back to top](#)

M

Malicious Software: Software, for example, a virus, designed to damage or disrupt a system.

Minimum Necessary: The least amount of information, when using or disclosing confidential client information that is needed to accomplish the intended purpose of the use, disclosure, or request.

Mission Critical: Activities, processing, etc., which are deemed vital to the organization's business success and, possibly, its very existence.

N

Non-routine Disclosure: A disclosure of records that is not for the purpose for which it was collected.

Non-routine Use: The use of records that is not for a purpose for which it was collected.

O

Open Office Environment: A work location structured with few enclosed offices or rooms in which private conversations may be conducted. An open office environment is characterized by individual work stations not separated by walls or partitions, or by partitions that do not extend from floor-to-ceiling or have a closable door and therefore do not allow for workstation conversations that cannot be overheard by other persons.

[Back to top](#)

P

Participant: Individuals participating in Department population-based services, programs, and activities that serve the general population, but who do not receive program benefits or direct services received by a client. Examples of participants include but are not limited to an individual whose birth certificate is recorded with Department of Vital Statistics, the subjects of public health studies, immunization or cancer registries, newborn screening, and other public health services, and individuals who contact Department hotlines or the ombudsman for general public information services.

Password: Confidential authentication information composed of a string of characters.

Patch: Vendors, in response to the discovery of security vulnerabilities, provide sets of files that have to be installed on computer systems. These files 'fix' or 'patch' the computer system or programs and remove the security vulnerability.

Payment: Any activities undertaken by the Department related to a client to whom health care is provided in order to:

- Obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the Medicaid Program or other publicly funded health care services;
- Obtain or provide reimbursement for the provision of health care.
- Payment activities include:
 - Determinations of eligibility or coverage, including coordination of benefits or the determination of cost sharing amounts, and adjudication of health benefit or health care claims;
 - Risk adjusting amounts due which are based on enrollee health status and demographic characteristics;
 - Billing, claims management, collection activities, obtaining payment under a contract for reinsurance, and related health care data processing;
 - Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
 - Utilization review activities, including pre-certification and pre-authorization of services, concurrent and retrospective review of services; and
 - Disclosure to consumer reporting agencies of any of the following information relating to collection of premiums or reimbursement: name and address; date of birth; payment history; account number; and name and address of the health care provider or health plan.

Personal Representative: A person who has authority to act on behalf of an individual in making decisions related to health care.

Physical Safeguards: Physical measures, policies and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards and unauthorized intrusion.

Privacy: An individual's or organization's right to determine whether, when and to whom personal or organizational information is released. Also, the right of individuals to control or influence information that is related to them, in terms of who may collect or store it and to whom that information may be disclosed.

Privacy Rights: The specific actions that an individual can take or request to be taken with regard to the uses and disclosures of their information.

Protected Health Information (PHI): Any individually identifiable health information, whether oral or recorded in any form or medium that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. Any data transmitted or maintained in any other form or medium by covered entities, including paper records, fax documents and all oral communications, or any other form, such as screen prints of eligibility information, printed e-mails containing identified individual's health information, claim or billing information, hard copy birth or death certificate. PHI does not include: school records that are subject to the Family Educational Rights and Privacy Act; and employment records held in the Department's role as an employer.

Protected Information: Any participant or client information that the Department may have in its records or files that must be safeguarded pursuant to Department policy. This includes but is not limited to "individually identifying information".

Provider: A person or entity that may seek reimbursement from the Department as a provider of services to Department clients pursuant to a contract. For purposes of these rules, reimbursement may be requested on the basis of claims or encounters or other means of requesting payment.

Psychotherapy Notes: Notes recorded in any medium by a health care provider who is a mental health professional documenting or analyzing the contents of conversations during a private counseling session, or group, joint, or family counseling session, when the notes are separated from the rest of the individual's record. Psychotherapy notes do not include medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, treatment plan, symptoms, prognosis, and progress to date.

Public Official: Any employee of a government agency, including but not limited to DHS, who is authorized to act on behalf of that agency in performing the lawful duties and responsibilities of that agency.

Public Health Agency: A public agency, including the Department, or a person or entity acting under a grant of authority from or by contract with the Department or public agency that performs or conducts one or more of the following essential functions that characterize public health programs, services, or activities:

- Monitor health status to identify community health problems;
- Diagnose and investigate health problems and health hazards in the community;
 - Inform, educate, and empower people about health issues;
 - Mobilize community partnerships to identify and solve health problems;
 - Develop policies and plans that support individual and community health efforts;
 - Enforce laws and regulations that protect health and ensure safety;
 - Conduct individuals to needed personal health services and assure the provision of health care when otherwise unavailable;
 - Ensure a competent public health and personal health care workforce;
 - Evaluate effectiveness, accessibility, and quality of personal and population-based health services; and
 - Perform research for new insights and innovative solutions to health problems.

Public Health Authority: An agency or authority of the United States, a State, territory, political subdivision of a State or territory, Indian tribe, or a person or entity acting under a grant of authority from or by contract with the public agency, including the employees or agents of the public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate. When performing functions as a Public Health Agency, the Department acts as a Public Health Authority for purposes of these rules.

[Back to top](#)

R

Re-disclosure: The disclosure of information to a person, a Department program, Department subcontracted entity, or other entity beyond what was originally authorized or to someone other than originally authorized.

Remote Log In: If an end-user uses a network to log in to a system, this act is known as remote log in.

Research: A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalized knowledge.

Required by Law: A duty or responsibility that federal or state law specifies that a person or entity must perform or exercise. Required by law includes but is not limited to court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or rules that require the production of information, including statutes or rules that require such information if payment is sought under a government program providing public benefits.

Routine and Recurring Disclosure: The disclosure of records for a purpose that is compatible with the purpose for which the information was collected.

S

Security/Security Measures: Encompass all of the administrative, physical and technical safeguards in an information system.

Security Incident: The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Server: A server is a computer system, or a set of processes on a computer system providing services to clients across a network.

Shared Account: A common account is shared by a group of users as opposed to a normal account, which is available to only one user. If the account is misused, it is very difficult or impossible to know which of users was responsible.

Specially Protected Records: Health records that have more stringent federal or state confidentiality requirements than HIPAA.

Storage System: Any form of office equipment or furniture, including but not limited to file cabinets, lateral files, or shelving units, in which a DHS office stores client information or files.

Systems Administrator: The individual who maintains the system and has system administrator privileges. In order to avoid errors and mistakes done by this individual while not acting as an administrator, he/she should limit the time he/she acts as an administrator (as known to the system) to a minimum.

[Back to top](#)

T

Technical Safeguards: The technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

Threats: The potential that an existing vulnerability can be exploited to compromise the security of systems or networks. Even if vulnerability is not known, it represents a threat by this definition.

Treatment, Payment and Operation (TPO): Please refer to the separate definitions for Treatment, Payment and Health care operations.

Treatment: The provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with the third party; consulting between health care providers relating to a patient or

the referral of a patient for health care from one health care provider to another.

U

Use: The sharing of individual information within a Department program or the sharing of individual information between program staff and administrative staff that support or oversee the program.

User: A person or entity with authorized access.

V

Virus: A program, which replicates itself on computer systems by incorporating itself (secretly and maliciously) into other programs. A virus can be transferred onto a computer system in a variety of ways.

Vulnerability: Vulnerability is the existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the system, network, application, or protocol involved.

Virus-Detection Tool: Software that detects and possibly removes computer viruses, alerting the user appropriately.

W

Workstation: An electronic computing device, for example a laptop or desktop computer, or any other device that performs similar functions and electronic media stored in its immediate environment.

Worm: A computer program, which replicates itself and is self-propagating. Worms, as opposed to viruses, are meant to spawn in network environments.