# Glossary

**Aggregate data:** Communitywide data that are de-identified and can be used for analytical purposes.

**Annual progress report (APR):** A standard Federal reporting form used by the U.S. Department of Housing and Urban Development for CoC homeless grant programs.

**Antivirus programs:** Computer programs that detect and rid computer systems of electronic viruses and thus prevent and/or mitigate file corruption and data loss.

**Application service provider (ASP):** A company that provides a range of computer application services, including hosting software applications. Clients access the software via the Internet, often using a secure connection. In this model, the ASP is responsible for maintaining and upgrading the software on an ongoing basis.

**Application software:** Computer programs designed to accomplish specific tasks or transactions. HMISs are application software.

**Application virus:** A program written to damage or otherwise adversely affect a computer system and its operations. Viruses can propagate through networks, floppy disks, e-mail, and so forth, and are designed to be difficult to detect.

**Audit trail:** A system that monitors, records, and reports on the activities of computer program end users.

**Back end:** The server portion of the HMIS, which provides supporting technology. This technology is normally inaccessible to end-users and is more tightly controlled because it contains all of an HMIS's data.

**Batch system structure:** A network structure that allows program sites to upload (transfer) data to a central data repository periodically (in batches) where they are aggregated with data from other programs.

**Central server:** A computer or group of computers that contains the main application software or aggregate data in a distributed HMIS.

**Central server organization:** The organization that manages, maintains, and monitors HMIS data and operations. This organization usually provides ongoing technical assistance to participating agencies.

**Certificate authority:** A third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs. The Certificate Authority guarantees that the individual granted the unique certificate is, in fact, whom he/she claims to be. Certificate Authorities are critical to data security and electronic commerce because they guarantee that the two parties exchanging information are whom they claim to be.

**Client computer:** The equipment that the end user utilizes to access the HMIS, also called a workstation. Most often referred to as a desktop personal computer, it is normally connected to a server to access information.

**Client confidentiality:** Except as provided by law or incorporated in properly executed consent, a client's right to guaranteed privacy of the personal information that is stored within the HMIS.

**Client consent:** Oral permission to participate in the HMIS (or, in the case of information that is required by program funders, acknowledgment that the information is being collected, stored, and aggregated for reporting purposes within the HMIS). Written consent is written permission to share personal information that is stored in the HMIS with another agency. The HMIS client consent form should explicitly state how the data will be collected, shared, and used, and explain a client's right to protect and limit its use.

**Client-level data:** Data about an individual HMIS client.

**Client/server system:** Architecture in which the client and server computers are connected via a LAN or WAN. The client computer handles the user interface and may perform some or all of the application processing. A database server maintains the databases and processes requests to extract data or update the database.

**Communications server:** A dedicated server that remote users can connect to through communications devices such as modems.

**Computer operating systems:** Computer programs that manage end user interaction with the system. Microsoft Windows is an example of an operating system.

**Computer networking:** The process of connecting multiple computers to facilitate easy sharing of files or programs. Networked computers can share common resources such as a printer or a database.

**Concurrent users:** The number of computer users accessing a system simultaneously.

**Connectivity:** The technology used to upload/download data files to/from other computers or to link to the Internet.

**Consent form:** The consumer's written authorization to have their data input in an HMIS and/or shared with other agencies.

**Consumer(s):** An individual or family experiencing homelessness, threatened with the imminent prospect of homelessness, or with a former experience of homelessness, **and** accessing services within the CoC.

**Continuum of Care (CoC):** A coordinated approach at the local level to deliver services to persons who are homeless. A CoC generally includes a full range of emergency, transitional, and permanent housing and service resources to address the various needs of homeless persons. HUD issues an annual Notice of Funding Availability (NOFA), known as the CoC grant, to local communities for housing and service funds.

**Coverage:** The proportion of shelter users that is represented in the data.

**Customization:** The extent to which a software program can be modified to meet a particular local or program need.

**Cutover startup:** Replacing an existing automated or manual system with a new HMIS at one point in time. The old system is removed and the new system begins operation instantaneously.

**Database:** A collection of information organized so that a computer program can quickly select desired pieces of data. You can think of a database as an electronic filing system.

**Database administrator (DBA):** The personnel responsible for monitoring, maintaining, and servicing HMIS data files.

**Database applications:** A class of computer programs (DBMS) that manage large amounts of data.

**Data conversion/migration:** The process of moving data from one data system to another.

**Data dictionary:** A document that defines data elements.

**Data encryption:** The conversion of plain text into masked data by scrambling it using a secret code that hides its meaning to any unauthorized viewer. Computers encrypt data by using algorithms or formulas. Encrypted data are not readable unless they are converted back into plain text via decryption.

**Data sharing agreement:** An agreement among participating agencies about the sharing of consumer data. The agreement should define which agencies will share what data elements under what particular circumstances.

**Data warehouse:** A system for storing, retrieving, and managing large amounts of data. Data warehouses contain a wide variety of data that present a coherent picture of conditions at a single point in time.

**Disaster and recovery:** Services involved in planning and preparing for contingencies to address HMIS continuity during catastrophes. Preparation can include setting up onsite and off-site backup systems, a change-over process when a backup server is needed, backup power supply and communication link preparedness, and recovery of lost data.

**Distributed architecture:** Systems designed utilizing a distributed architecture share resources among multiple computers. An HMIS based on this model functions over a LAN, a WAN, or the Internet.

**End user:** The participating agency staff person who will be using the HMIS to enter and/or extract data.

**Extranet:** The extension of an organization's intranet onto the Internet to allow selected members of the public to access the organization's private data and applications.

**Firewall:** A hardware and/or software system that enforces access control between two networks.

**Front end:** The portion of a HMIS with which the end user interacts.

**Function:** The specific capabilities or features that the HMIS performs.

**Generalize:** The extent to which information on a sample can be used to describe the general population.

**HIPAA:** The Health Insurance Portability & Accountability Act of 1996. Specifically, this law calls for the standardization of electronic patient health, administrative, and financial data; unique health identifiers for individuals, employers, health plans, and healthcare providers; and security standards protecting the confidentiality and integrity of "individually identifiable health information," past, present, or future.

**Homegrown:** A software program developed for a local community, not a commercially available product.

**Homeless Management Information System (HMIS):** A computerized data collection system that stores information about persons experiencing homelessness, collected throughout the community from the various agencies that provide services to these individuals. Client-level information collected from each program can be aggregated with data from other programs using a unique client identifier to determine unduplicated systemwide information, such as the overall level of homelessness, service effectiveness, and unmet community needs.

**Host:** A computer system or organization that plays a central role, normally providing data storage and/or application services to participating agencies. Many HMIS software providers offer this service as an option for communities that do not have the expertise or prefer not to store the information locally.

**Information and referral:** Electronic databases of local resources.

**Internet service provider (ISP):** Any company that provides individuals or organizations with access to the Internet.

**Intranet:** A network or group of networks communicating with each other using Internet technology. An intranet is often used within agencies for internal communication, and is only available to an organization's staff, as opposed to customers or the general public.

**Local area network (LAN):** A network that is geographically limited, allowing easy interconnection of computers within offices or buildings.

**Logon process:** The procedure by which a computer network authenticates a user.

**Longitudinal data:** Information collected about particular individuals over time.

**Modem:** A data communications device that transforms digital signals to analog, transmits the analog signals over conventional telephone lines, and carries out the reverse transformation at the destination, to enable remote computer communications.

**Network:** Several computers or computer systems linked to one another.

**Network administration:** The personnel responsible for setting up, operating, and maintaining the HMIS data communications network.

**Outsourcing:** The practice of contracting out a component or all system operations and maintenance to a third party.

**Parallel startup:** Running both old and new systems simultaneously for a period of time, during which results are compared. When users are comfortable that the new system is working correctly, the old system is eliminated.

**Participating agency:** An agency that operates an HMIS.

**Phase-in startup:** Slowly replacing components of the old system with those of the new one; this process is repeated for each portion of the HMIS until the new system is running and performing as expected.

**Pilot startup:** Running the new system for a subgroup of users rather than all users.

**Productivity tools:** Computer programs said to increase the efficiency of office workers such as word processing, spreadsheet, and database management programs.

**Public key infrastructure:** A system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction. (See Certificate Authority.)

**Real-time:** Pertaining to the current moment. Technology that allows a user to receive data during the actual time that it is entered into the system.

**Record-level encryption:** Data encryption that occurs at the field (data element) level within an information record.

**Replacement factor:** An estimation of the number of current personal computers that require substitution or significant upgrade.

**Representative:** The extent to which the data reflect the population served.

**Request for proposal (RFP):** A process used to solicit applications to provide a particular service or product.

**Robustness (database):** Refers to a product or a system that holds up well under exceptional conditions. Robust software products have very low failure rates.

**Seat:** A computer workstation.

**Secure Socket Layer (SSL) protection:** A communications protocol used to secure sensitive data. SSL is normally described as wrapping an encrypted envelope around message transmissions over the Internet.

**Security:** Absolute protection of the client and program information stored in the HMIS from unauthorized access, use, or modification.

**Security probe:** Commonly referred as "penetration testing," consists of actively testing various aspects of the HMIS's network security. Results are used to suggest future security improvements.

**Server computer:** A computer that provides a service for other computers connected to it via a network. Servers can host and send files, data, or programs to client computers.

**Site:** A location that uses an HMIS and at which services to homeless and at-risk consumers are provided.

**Site preparation:** Preparation for installation of a new HMIS.

**Software license:** The right of an organization or individual to use or access a computer program developed by a third party, for a fee.

**Software license agreement:** Agreement between the developer of a software product and its users that specifies the rules under which software distribution, installation, and usage can occur.

**Software release:** A version of a software product that is available on the market.

**Standard operating procedures (SOPs):** Standard methods for conducting tasks or processes, documented to ensure consistency among all participants.

**Structured query language (SQL):** A database language used to manipulate relational databases. SQL was adopted as an industry standard in 1986.

**Systems implementation:** A stage in the HMIS project during which the various system components (hardware, software, databases, etc.) are created or acquired, assembled, and put into operation.

**Technical capacity:** The documented sets of technical skills and resources available for undertaking an HMIS project.

**Technical requirements:** The documented sets of technical skills and resources necessary for undertaking an HMIS project.

**Two-tier/three-tier:** Client/server architecture in which the user interface runs on the client computer and the database is stored on the server. The actual processing can occur on either the client or the server computer. Newer client/server architecture, known as three-tier, introduces a middle tier where the processing occurs.

**Undisclosed locations:** Sites, such as shelters for victims of domestic violence, which have chosen to hide their location in order to protect program consumers.

**Unique client identifier (ID):** A code associated with a single individual that can be used to create an unduplicated client count, but which cannot be used to identify that individual.

**Vendor developed:** A commercially developed software system.

**Web browser:** Software that provides a graphical interface to the Web.

**Web-enabled application:** Application software designed to operate as an Internet application. Users access the system with a Web browser such as Netscape or Internet Explorer.

**Web server:** A computer that delivers (serves up) Web pages.

**Wide area network (WAN):** A network that is not geographically limited, and can link computers in different locales and extend over large distances. A WAN is often used to connect computers that are not located in the same office or building.

**World Wide Web (WWW):** An Internet information management system. On the WWW, all information is represented to the user as a hypertext object in HTML format. The client program, or browser, runs on the user's computer and provides basic navigation, data entry, and validation.