Student Data Privacy – Glossary of Terms

Passwords - A password is a string of characters used for authenticating a user on a computer system. For example, you may have an account on your computer that requires you to log in. In order to successfully access your account, you must provide a valid username and password. This combination is often referred to as a login. While usernames are generally public information, passwords are private to each user.

Encryption - Encryption is the conversion of electronic data into another form, called ciphertext, which cannot be easily understood by anyone except authorized parties (those that have decryption keys)[i].

SSL - The Secure Sockets Layer (SSL) is a computer networking protocol that manages server authentication, client authentication and encrypted communication between servers and clients.

SSH - Stands for "Secure Shell." SSH is a method of securely communicating with another computer.

HTTPS (also called HTTP over TLS, HTTP over SSL and HTTP Secure) - is a protocol for secure communication over a computer network which is widely used on the Internet. HTTPS consists of communication over Hypertext Transfer Protocol (HTTP) within a connection encrypted by Transport Layer Security or its predecessor, Secure Sockets Layer. The main reason for using HTTPS is authentication of the visited website and protection of the privacy and integrity of the exchanged data.

Cloud - Cloud computing refers to applications and services offered over the Internet. These services are offered from data centers all over the world, which collectively are referred to as the "cloud." This metaphor represents the intangible, yet universal nature of the Internet.

Protected health information (PHI) - under US law is any information about health status, provision of health care, or payment for health care that is created or collected by a "Covered Entity" (or a Business Associate of a Covered Entity), and can be linked to a specific individual. This is interpreted rather broadly and includes any part of a patient's medical record or payment history.

PHI is often sought out in datasets for de-identification before researchers share the dataset publicly. When researchers remove PHI from a dataset they do so in an attempt to preserve privacy for research participants.

Personally Identifiable Information (PII) - NIST Special Publication 800-122 defines PII as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." So, for example, a user's IP address as used in a communication exchange is classed as PII regardless of whether it may or may not on its own be able to uniquely identify a person.

De-identification is the process used to prevent a person's identity from being connected with information. Common uses of de-identification include human subject research for the sake of privacy for research participants.

Chief Privacy Officer (CPO) is a senior level executive within a business or organization. "Consumer concerns over the use of personal information, including medical data and financial information along with laws and regulations", is one of the key reasons that the CPO role exists, as this was introduced to help keep personal information safe.

[i] Sources http://techterms.com/, https://en.wikipedia.org and http://www.nist.gov/