Common terms: Data protection and HIPAA compliance

Administrative safeguards: The mechanisms required to protect electronic systems, equipment and the data they hold from threats, environmental hazards and unauthorized intrusion. They include restricting access to electronic protected health information (ePHI) and retaining offsite computer backups.[1]

Backup: A copy of data, as it existed at a specific point in time, that can be used to restore the original after a data loss event.

Business associate: A business associate is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. A covered entity must have a written business associate contract or other arrangement with the business associate that establishes specifically what the business associate has been engaged to do and requires the business associate to comply with HIPAA regulations. In addition to these contractual obligations, business associates are directly liable for compliance with certain provisions of the HIPAA Rules. A member of the covered entity's workforce is not a business associate. Examples of business associates include, but are not limited to: claims processing or administration; data analysis, processing or administration; billing, legal or data handling.[2]

Contingency plan: Management policies and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of an emergency, system failure or disaster.[3]

Covered entity: Individuals, organizations and agencies that must comply with HIPAA requirements to protect the privacy and security of health information and provide individuals with certain rights with respect to their health information. Covered entities include, but are not limited to: health care providers, health care clearinghouses and health plans.

Disaster recovery plan: A series of processes and tools, as part of a contingency plan, that focus specifically on the data recovery process. For example, using an on-site backup appliance as well as cloud storage to restore data either on-site or at an alternate location.[4]

Encryption: The process of encoding information into an unrecognizable or "encrypted" form, so that only authorized parties can read it.

Electronic communications: Any message or information that is transmitted electronically. Examples of electronic communication include, but are not limited to: phone calls, texts, email, websites, apps and faxes.

Electronic health record (EHR): An electronic record of health-related information on an individual that is created, held or maintained by a health care provider and may contain all the information that once existed in a patient's paper medical record, but in electronic form.[5]

HIPAA: Health Insurance Portability and Accountability Act of 1996

Common terms: Data protection and HIPAA compliance

HIPAA security rule: HIPAA requires that both covered entities and business associates implement administrative, physical and technical safeguards only for electronic PHI.

Network service provider (NSP): A business or organization that sells bandwidth or network access to the internet. Network service providers may include, but are not limited to: telecommunications companies, data carriers, wireless communications providers, internet service providers and cable television operators offering high-speed internet access.

Physical safeguards: 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.[6]

Privacy rule: HIPAA requires that all covered entities limit uses and disclosures of all protected health information (PHI) and implement safeguards in order to protect the confidentiality of all PHI.

Protected heath information (PHI): Any identifiable health information collected from an individual that is transmitted or maintained in any form or medium by a covered entity or its business associate. Health information includes: demographic information, information on an individual's physical or metal health, the provision of or payment for health care, or information that could be used to identify the individual in any way. PHI does not include employment records, or Family Educational Rights and Privacy Act (FERPA) records.[7]

Remote access: A method of gaining access to a computer or network from a remote location using software or an operating system feature.

Risk analysis: An accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information held by the covered entity.[8]

SSH: "Secure Shell," or SSH, is an encrypted network protocol that allows a user to safely log in to a network remotely. Any network service can be secured with SSH.

System: Any electronic or internet-connected device or application that can create, access, transmit or receive protected health information. Examples of systems include, but are not limited to: computers, mobile phones, voicemail, databases, servers, printers and fax machines.

System administrator (sysadmin): A person who is responsible for managing, maintaining and overseeing networked computers and servers within a business or organization.

Technical safeguards: The technology, and the policy and procedures for its use, that protect electronic protected health information and control access to it.[9]

Transport layer security (TLS): Transport layer security and its predecessor, secure sockets layer (SSL), are cryptographic protocols that provide communications security over a computer network.

Find out how Carbonite can support your HIPAA compliance efforts today.

Source:
[1]Centers for Medicare & Medicaid Services, Security 101 for Covered Entities
[2]http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/
[3]http://www.hhs.gov/ocio/eplc/EPLC%20Archive%20Documents/36-Contingency-Disaster%20Recovery%20Plan/eplc_contingency_plan_practices_guide.pdf
[4]http://www.hhs.gov/ocio/eplc/EPLC%20Archive%20Documents/36-Contingency-Disaster%20Recovery%20Plan/eplc_contingency_plan_practices_guide.pdf
[5]http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/phrs.pdf
[6]http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf
[7]http://www.hhs.gov/ocr/privacy/hipaa/understanding/training/udmn.pdf
[8]http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf
[9]http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf