Appendix A: Definitions

Term	Definitions
Business Associate	A Contractor who completes a function or activity involving the use or disclosure of protected health information (PHI) or electronic protected health information (EPHI) on behalf of a HIPAA covered component. Services that Business Associate (BA) contractors provide include: Claims processing or administration; data analysis, processing and/or administration; data analysis, processing and/or administration; utilization review; quality assurance; billing; benefit management; document destruction; temporary administrative support; legal; actuarial; accounting; consulting; information technology (IT) support. The BA contractor does not deliver health care services to clients of the HIPAA covered component.
Breach	An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised.
Device	A unit of hardware, inside or outside the case or housing for the essential computer functions (the processor, memory, and data paths). A device is capable of providing input, receiving output, or both.
Dial Up	Dialing in to an internet service provider over a modem and phone line.
Disposal	The removal or destruction of electronic protected health information from electronic media.
DMZ (demilitarized zone)	Any untrusted network connected to, but separated from, **Saratoga Bridges**'s corporate network by a firewall, used for external (Internet/partner, etc.) access from within **Saratoga Bridges**, or to provide information to external parties.
Electronic Protected Health Information (EPHI)	Protected Health Information (PHI) is health information that a covered entity creates or receives that identifies an individual, and relates to: The individual's past, present, or future physical or mental health or condition; the provision of health care to the individual; or the past, present, or future payment for the provision of health care to the individual. EPHI is such information in electronic format such as: information system applications; internet, intranet and extranet; email; USB drives; computer screens; laptops; storage devices (magnetic tapes, floppy disks, CDs, optical devices).
Email	The electronic transmission of information through a mail protocol such as SMTP. Programs such as Eudora and Microsoft outlook use SMTP.
Encryption	A method of scrambling or encoding electronic data to prevent unauthorized access. Only individuals with access to a password or key can decrypt (unscramble) and use the data.
Facility	A building, owned or leased, in which the workforce accesses Electronic Protected Health Information (EPHI).
Firewalls	Special computer programs and hardware that are set up on a network to prevent an intruder from stealing or destroying data.

Forwarded email	Email re-sent from internal networking to an outside point.
Hard Drive	An information storage device that contains electronic information and software programs on a computer. Information stored on the hard drive [or local (C:) drive] is not backed up on the network.
IT	Information Technology. Refers to the Management Information Systems department or the Information Technology staff at **Saratoga Bridges**.
Jailbreak	To remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorized software.
Key pads - cipher locks	Door locks that require a combination of numbers entered into a pad in order to unlock the door.
Local (C:) drive	In the context of this policy, the individual user's hard drive where electronic information can be stored (saved), rather than stored on the organization-wide network. The local (C :) drive should not be used to store EPHI.
Malicious software or malware	A type of software that includes ways of attacking data integrity, the system itself or the confidentiality of the data. Malicious software includes viruses, virus variants, worms, hoaxes, and Trojan horses.
Media reuse	A device such as a computer hard drive that contained data (information) that is being reused to contain new data.
Modem	A device that enables data to be transmitted over telephone or cable lines. It translates telephone tones to allow for the multiplexing of data (information) across the telephone network, generally in order to access the internet.
Network	A group of computers (workstations) and associated devices connected by a communications channel to share information files and other resources between multiple workforce members.
Network closets	Storage area of network equipment such as hubs, routers, switches, racks, cables, and sometimes has telephone equipment, at a HIPAA covered component facility.
Networked computer/workstation	A workstation computer that uses server resources. It is usually connected to a Local Area Network (LAN), which shares the resources of one or more large computers.
Payload	Harmful code delivered by a software virus.
Perimeter Security	Security that protects the network and its component server computers from attack or intrusion.
Portable media	Devices carried or moved with ease that can contain electronic protected health information (EPHI). The most common are: laptops; CDs; USB drives (or memory sticks); and personal digital assistants (PDAs), including smartphones or Blackberries.

Risk Assessment	A process of assessing those factors that could affect confidentiality, availability, and integrity of key information assets and systems. HIPAA covered components are responsible for ensuring the integrity, confidentiality, and availability of EPHI and equipment that contains it, while minimizing the impact of security procedures and policies upon business productivity.
Secure Channel	Out-of-band console management or channels using strong encryption according to the ***Acceptable Encryption Policy***. Non-encrypted channels must use strong user authentication (one-time passwords).
Sensitive information	Information is considered sensitive if it can be damaging to **Saratoga Bridges** or its customers' dollar value, reputation, or market standing.
Server	A computer or device on a network that managers network resources.
Server Room	The room where all the server computers are housed.
Strong Passwords	A password that is difficulty to guess by both humans and computer programs, effectively protecting data from unauthorized access. A strong password consists of at least six characters that are a combination of letters, numbers and symbols (@, #, $, %, etc.) if allowed. Strong passwords contain the maximum number of characters allowed. Passwords are typically case-sensitive so a strong password contains letters in both uppercase and lowercase. Strong passwords also do not contain words that can be found in a dictionary or any part of the user's own name.
Transmitting	The act of sending a message or data using an electronic medium.
Trojan or Trojan horse	A Trojan or Trojan horse is a computer program generally designed to impact the security of a network system. The Trojan is usually disguised as something else (a benign program) or masquerades as a legitimate file that the user would expect to see, or want to load, on the network system. The payload of a Trojan is usually delivered as soon as it is opened with devastating results. Trojans often create "back doors" that allow access into a secure network. A hacker can then gain access to the secure network. Trojans are most often delivered as an attachment to a seemingly innocent chain email.
Unauthorized Disclosure	The intentional or unintentional revealing of restricted information to people who do not have a need to know that information.
Un-trusted Network	Any network firewalled off from the corporate network to avoid impairment of production resources from irregular network traffic (lab networks), unauthorized access (partner networks, the Internet, etc.) or anything else identified as a potential threat to those resources.
USB drive, USB flash drive, thumb drive, or memory stick	A small, portable device that plugs into a workstation computer's USB port and functions as a portable hard drive with extra storage capacity. USB devices are easy to use, small enough to be carried in a pocket, and can plug into any workstation computer with a USB drive.

User	For the purposes of this document, any workforce member (permanent or temporary), contractor, consultant, vendor, volunteer, student, or other person who uses, maintains, manages, or is otherwise given access privileges to system resources.
User ID or logon	An identification code issued for access privileges which identifies the user to IT systems.
Virtual Private Network (VPN)	A secure, encrypted network connection between two or more devices across the public internet or other shared network. It allows workstation computers at different locations to securely communicate with each other.
Virus	A computer program that copies itself into another program, sectors on a drive, or into items that support scripts. A virus may unleash a payload. Payloads can damage files, corrupt hard drives, display messages, or open other files. Typically, the payload is delivered when a certain condition occurs, such as when the date on the workstation reaches a particular day.
Workforce/ workforce member	In the HIPAA Privacy rule, the term "workforce" is defined as "employees, volunteers, trainees, and other persons who conduct, in the performance of work for a HIPAA covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity." Workforce members include supervisors, managers, and staff.
Workstation	A laptop or desktop computer, or any other device that performs computer functions.
Worm	A type of virus that finds vulnerable computer systems and then copies itself into those systems. The most frequent copying methods are from email distribution lists, email signature scripts, and shared folders on the network. A typical worm payload makes the workstation more susceptible to other malicious viruses.