HIPAA GUIDELINES AND CYBERSECURITY:

DO YOU KNOW THE ANSWERS TO THESE FOUR QUESTIONS VITAL TO THE SECURING OF PHI AND ePHI?

THE SATURN PARTNERS, INC.
Network and Environmental Security Auditing

9155 Lakeshore Drive, Pleasant Prairie, WI 53158
PHONE: (262) 942.3626 FAX: (262) 694.8205
EMAIL: cacraw@saturnpartners.com
WEBSITE: www.saturnpartners.com

HIPAA GUIDELINES AND CYBERSECURITY:

DO YOU KNOW THE ANSWERS TO THESE FOUR QUESTIONS VITAL TO THE SECURING OF PHI AND ePHI?

What is the difference between the terms "HIPAA Compliant" and "HIPAA Alignment?"

At The Saturn Partners, Inc., many of the services used to assist health care clients are managed using standards-based data security practices that make it possible (with proper precautions) for our engineers to handle and store electronic protected health information (ePHI) and other sensitive data regulated by the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. These systems and services are designated "HIPAA-aligned" and not "HIPAA-compliant", because the latter term is an official designation applicable only to certified US federal agencies.

SPI's HIPAA alignment effort on behalf clients is based on IT management processes compatible with security best practices standards, specifically National Institute of Standards and Technology (NIST) Special Publication 800-53, as recommended by US Department of Health and Human Services, which oversees HIPAA regulation.

THE SATURN PARTNERS, INC.
Network and Environmental Security Auditing

9155 Lakeshore Drive, Pleasant Prairie, WI 53158
PHONE: (262) 942.3626 FAX: (262) 694.8205
EMAIL: cacraw@saturnpartners.com
WEBSITE: www.saturnpartners.com

Which data elements in the classifications of institutional data are considered protected health information (PHI)? Think of a University hospital, for example:

The data elements listed on the Classifications of Institutional Data page may or may not constitute PHI, based on the context. The following table clarifies this by providing a list of data elements that do or may constitute PHI; any data element not appearing in the list below is not PHI.

Data element	Classification	Is data containing the element PHI?
Health information - Fax numbers	Critical	PHI
Health information - Email address	Critical	PHI
Health information - Medical record numbers	Critical	PHI
Health information - Health plan beneficiary numbers	Critical	PHI
Health information - Account numbers	Critical	PHI
Health information - Certificate/license numbers	Critical	PHI
Health information - Device identifiers	Critical	PHI
Health information - URLs, IP addresses	Critical	PHI
Health information - Biometric identifiers	Critical	PHI
Health information - Full face photographic images	Critical	PHI
Health information - Any other unique identifier	Critical	PHI
Health information - Telephone numbers	Critical	PHI
Health information - Names	Critical	PHI
Social Security number	Critical	PHI if it satisfies this definition
Driver's license number	Critical	PHI if it satisfies this definition
Passport number	Critical	PHI if it satisfies this definition
Visa number	Critical	PHI if it satisfies this definition
State identification card number	Critical	PHI if it satisfies this definition
Certificate/license number	Critical	PHI if it satisfies this definition

THE SATURN PARTNERS, INC.
Network and Environmental Security Auditing

9155 Lakeshore Drive, Pleasant Prairie, WI 53158
PHONE: (262) 942.3626 FAX: (262) 694.8205
EMAIL: cacraw@saturnpartners.com
WEBSITE: www.saturnpartners.com

DO YOU KNOW THE ANSWERS TO THESE FOUR QUESTIONS VITAL TO THE SECURING OF PHI AND ePHI?

Data element	Classification	Is data containing the element PHI?
All payment card data (including all credit/debit cards and cardholder information)	Critical	PHI if it satisfies this definition
Debit card number	Critical	PHI if it satisfies this definition
Bank account number or other financial account numbers	Critical	PHI if it satisfies this definition
Health information	Critical	PHI if it satisfies this definition; not PHI if it has been de-identified
Health information - Geographic information smaller than a state	Critical	PHI
Date of birth/age	Restricted	PHI if it satisfies this definition
Emergency contact	Restricted	PHI if it satisfies this definition
Home mailing address	Restricted	PHI if it satisfies this definition
Home phone	Restricted	PHI if it satisfies this definition
Visa status	Restricted	PHI if it satisfies this definition
Country of birth or citizenship	Restricted	PHI if it satisfies this definition
Work authorization (I-9)	Restricted	PHI if it satisfies this definition
Job action reason (e.g., terminations or leave)	Restricted	PHI if it satisfies this definition
Benefits enrollment info	Restricted	PHI if it satisfies this definition
Payroll information (e.g., taxes, deductions, etc.)	Restricted	PHI if it satisfies this definition
Marital status	Restricted	PHI if it satisfies this definition
Examples: Hospital ID, preferred name/prior name, position information, part-time/full-time indicator	University-internal	PHI if it satisfies this definition
Dates of first and last employment	Public	PHI if it satisfies this definition
Name	Public	PHI if it satisfies this definition
Compensation	Public	PHI if it satisfies this definition
Job title	Public	PHI if it satisfies this definition
Job description	Public	PHI if it satisfies this definition
Business address	Public	PHI if it satisfies this definition
Business telephone number	Public	PHI if it satisfies this definition
Previous work experience	Public	PHI if it satisfies this definition
Education and training background	Public	PHI if it satisfies this definition

THE SATURN PARTNERS, INC.
Network and Environmental Security Auditing

9155 Lakeshore Drive, Pleasant Prairie, WI 53158
PHONE: (262) 942.3626 FAX: (262) 694.8205
EMAIL: cacraw@saturnpartners.com
WEBSITE: www.saturnpartners.com

DO YOU KNOW THE ANSWERS TO THESE FOUR QUESTIONS VITAL TO THE SECURING OF PHI AND ePHI?

What four classification levels should any institution use as a guideline when handling sensitive data/PHI?

The Saturn Partners, Inc. uses the following classification levels which we recommend clients also use when handling sensitive data:

From most sensitive to least sensitive, the recommended data classifications are:

Critical	*Inappropriate handling of this data could result in criminal or civil penalties, identity theft, personal financial loss, invasion of privacy, and/or unauthorized access to this type of information by an individual or many individuals.*
Restricted	*Because of legal, ethical, or other constraints, may not be accessed without specific authorization, or only selective access may be granted.*
Internal	*May be accessed by eligible agents/directors/managers in the conduct of institutional/organization business; access restrictions should be applied accordingly.*
Public	*May be accessed by eligible agents/directors/managers in the conduct of institutional/organization business; access restrictions should be applied accordingly.*

THE SATURN PARTNERS, INC.
Network and Environmental Security Auditing

9155 Lakeshore Drive, Pleasant Prairie, WI 53158
PHONE: (262) 942.3626 FAX: (262) 694.8205
EMAIL: cacraw@saturnpartners.com
WEBSITE: www.saturnpartners.com

What encryption tools should you use for handling ePHI data "at rest" (stored) versus data "transfers?"

One tool The Saturn Partners recommends to encrypt at-rest ePHI and other HIPAA-regulated data, is GNU Privacy Guard (GPG, also GnuPG) . Here is what it is:

GnuPG is the GNU project's complete and free implementation of the OpenPGP standard as defined by RFC4880. GnuPG allows to encrypt and sign your data and communication, features a versatile key management system as well as access modules for all kinds of public key directories. GnuPG, also known as GPG, is a command line tool with features for easy integration with other applications. A wealth of frontend applications and libraries are available. Version 2 of GnuPG also provides support for S/MIME.

GnuPG is Free Software (meaning that it respects your freedom). It can be freely used, modified and distributed under the terms of the GNU General Public License.

GnuPG comes in two flavours: 1.4.16 is the well known and portable standalone version, whereas 2.0.23 is the enhanced and somewhat harder to build version.

Project Gpg4win provides a Windows version of GnuPG. It is nicely integrated into an installer and features several frontends as well as English and German manuals.

Project GPGTools provides a Mac OS X version of GnuOnePG. It is nicely integrated into an installer and features all required tools.

Project Aegypten developed the S/MIME functionality in GnuPG 2.

THE SATURN PARTNERS, INC.
Network and Environmental Security Auditing

9155 Lakeshore Drive, Pleasant Prairie, WI 53158
PHONE: (262) 942.3626 FAX: (262) 694.8205
EMAIL: cacraw@saturnpartners.com
WEBSITE: www.saturnpartners.com

On Personal Workstations:

On Windows and OS X workstations, to encrypt at-rest ePHI and other sensitive data, use PGP Whole Disk Encryption (WDE). For more information look these up:

- Encrypting your Windows computer with PGP Whole Disk Encryption
- Encrypting your Mac OS X computer with PGP Whole Disk Encryption

Important: Storing ePHI on laptops or other portable devices is highly discouraged. The HIPAA Security Rule mandates that ePHI data should not be stored on laptops, flash drives, external hard drives, or mobile devices, unless the data are anonymized or strongly encrypted!

Encrypting data transfers:
You can use SFTP (Secure FTP): See below!

To transfer ePHI and other HIPAA-regulated sensitive data between networked computers, use a Secure FTP (SFTP) client. SFTP clients encrypt commands and data to prevent sensitive information from being transmitted in the clear over a network.

What is it?

The SSH File Transfer Protocol (also known as Secure FTP and SFTP) is a computing network protocol for accessing and managing files on remote file systems. SFTP also allows file transfers between hosts, similar to the SCP protocol. Unlike standard File Transfer Protocol (FTP), SFTP encrypt commands and data both, preventing passwords and sensitive information from being transmitted in the clear over a network.

SFTP clients are programs that use SSH to access, manage, and transfer files. SFTP clients are functionally similar to FTP clients, but they use different protocols. Consequently, you cannot use standard FTP clients to connect to SFTP servers, nor can you use clients that support only SFTP to connect to FTP servers. Graphical clients are available for SFTP, or you can use it from the command line on a UNIX or Mac OS X computer.

THE SATURN PARTNERS, INC.
Network and Environmental Security Auditing

9155 Lakeshore Drive, Pleasant Prairie, WI 53158
PHONE: (262) 942.3626 FAX: (262) 694.8205
EMAIL: cacraw@saturnpartners.com
WEBSITE: www.saturnpartners.com

Graphical SFTP

These clients simplify file transfers by allowing you to drag and drop icons from one window to another. Each icon represents a file or directory, and each window represents a computer's file system. When you open the program, you specify the name of the remote host to which you want to connect, and then authenticate with your username and password for that host.

Command-line SFTP:

You can use SFTP from the command line on UNIX and Mac OS X computers. To start an SFTP session, at the command prompt, enter:

```
sftp username@host
```

For example, if your username is dvader, to connect to your account on the hostempire.gov, enter:

```
sftp dvader@empire.gov
```

Enter your password when prompted.

Some standard command-line SFTP commands include:

Command	Function
`cd`	Change the directory on the remote computer.
`chmod`	Change the permissions of files on the remote computer.
`chown`	Change the owner of files on the remote computer.
`exit (or quit)`	Close the connection to the remote computer and exit SFTP.
`get`	Copy a file from the remote computer to the local computer.
`help (or ?)`	Get help on the use of SFTP commands.
`lcd`	Change the directory on the local computer.
`lls`	List the contents of the current directory on the local computer.
`lmkdir`	Create a directory on the local computer.

THE SATURN PARTNERS, INC.
Network and Environmental Security Auditing

9155 Lakeshore Drive, Pleasant Prairie, WI 53158
PHONE: (262) 942.3626 FAX: (262) 694.8205
EMAIL: cacraw@saturnpartners.com
WEBSITE: www.saturnpartners.com

Command	Function
`ln (or symlink)`	Create a symbolic link for a file on the remote computer.
`lpwd`	Show the current directory (present working directory) on the local computer.
`ls (or dir)`	List the contents of the current directory on the remote computer.
`lumask`	Change the local umask value.
`mkdir`	Create a directory on the remote computer.
`put`	Copy a file from the local computer to the remote computer.
`pwd`	Show the current directory (present working directory) on the remote computer.
`rename`	Rename a file on the remote computer.
`rm`	Delete a file on the remote computer.
`rmdir`	Remove a directory on the remote computer (the directory usually has to be empty).
`version`	Display the SFTP version.
`!`	Exit to the Unix shell prompt, where you can enter commands. To get back to SFTP, enter exit. If you combine !with a command (e.g., !pwd), SFTP will execute the command without dropping you to the Unix prompt.

For More Information on HIPAA Compliance/Alignment or Securing ePHI and PHI in your network environment call us at The Saturn Partners at 262-942-3626, email us at cacrawf@saturnpartners.com or visit us at www.saturnpartners.com. Helping our clients become compliant and stay with HIPAA rules and regulations has been our business since 2001!

THE SATURN PARTNERS, INC.
Network and Environmental Security Auditing

9155 Lakeshore Drive, Pleasant Prairie, WI 53158
PHONE: (262) 942.3626 FAX: (262) 694.8205
EMAIL: cacraw@saturnpartners.com
WEBSITE: www.saturnpartners.com