



John Whatley  
Voice (770) 485-8954  
E-mail: [jwhatley@pssi-us.com](mailto:jwhatley@pssi-us.com)

*Personal Systems Services, Inc.*

3010 Eglantine Court  
Marietta, GA 30062-4988

[www.pssi-us.com](http://www.pssi-us.com)



Terry Gilbreath  
Voice (770) 587-9095 Fax (call first)  
E-Mail: [tgilbreath@pssi-us.com](mailto:tgilbreath@pssi-us.com)

---

## **PSSI's Expertise in Compliance & Security Requirements**

Over the years, PSSI has provided SMB clients with appropriate security remediation to meet their internal and external requirements. Security protection, like insurance, is one of the things you must have and hope you never have to use. But when an incident occurs, you'll be grateful you took the effort to plan for it in advance.

**The 2011 Data Breach Investigations Report states 92% of attacks discovered in 2010 were not highly difficult and there was a virtual explosion of breaches in 2010 of smaller organizations.**

The following are some of the areas in which PSSI has expertise:

1. PCI or PCI DSS Compliance
2. HIPPA Compliance
3. HITECH Act

### **PCI or PCI DSS Compliance** (Payment Card Industry Data Security Standard)

PCI DSS requirements must be implemented by all entities that store, process, or transmit payment cardholder data. In the event of a security breach, any entity which was not PCI DSS compliant at the time of breach will be subject to additional penalties or fines.

A quarterly vulnerability scan with a PCI SSC Approved Scanning Vendor (ASV) is required for Validation Type 4/5 merchants, which is any merchant computer with internet access. If you electronically store any cardholder information and have internet access, scanning is required.

In addition, guidelines apply to the deployment of Wireless Local Area Networks (WLANs) in Cardholder Data Environments, also known as CDEs. A CDE is defined as a network environment that possesses or transmits credit card data.

For more information:

[https://www.pcisecuritystandards.org/documents/pci\\_dss\\_v2.pdf](https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf)

PCI DSS includes 12 requirements that specify the framework for a secure payments environment; for purposes of PCI compliance, their essence is three steps: **Assess, Remediate** and **Report**.

**Assess** takes an inventory of your IT assets and business processes for payment card processing and analyze them for vulnerabilities that could expose cardholder data. **Remediate** is the process of fixing those vulnerabilities. **Report** entails compiling records required by PCI DSS to validate remediation and submitting compliance reports to the acquiring bank and global payment brands you do business with. Carrying out these three steps is an ongoing process for continuous compliance with the PCI DSS requirements. These steps also enable vigilant assurance of payment card data safety.

### ***Step 1 – Assess***

The primary goal of assessment is to identify all technology and process vulnerabilities that pose risks to the security of cardholder data that is transmitted, processed or stored by your business. Study the [Payment Card Industry Data Security Standard \(PCI DSS\)](#) PCI DSS for detailed

requirements. It describes IT infrastructure and processes that access the payment account infrastructure. Determine how cardholder data flows from beginning to end of the transaction process – including PCs and laptops that access critical systems, storage mechanisms for paper receipts, etc. Check the versions of personal identification number (PIN) entry terminals and software applications used for payment card transactions and processing to ensure they have passed PCI compliance validation.

Note: your liability for PCI compliance also extends to third parties involved with your process flow, so you must also confirm that they are compliant. Comprehensive assessment is a vital part of understanding what elements may be vulnerable to security exploits and where to direct remediation.

### ***Step 2 – Remediate***

Remediation is the process of fixing vulnerabilities – including technical flaws in software code or unsafe practices in how an organization processes or stores cardholder data. Steps include:

- Scanning your network with software tools that analyze infrastructure and spot known vulnerabilities
- Review and remediation of vulnerabilities found in on-site assessment (if applicable) or through the Self-Assessment Questionnaire process
- Classifying and ranking the vulnerabilities to help prioritize the order of remediation, from most serious to least serious
- Applying patches, fixes, workarounds, and changes to unsafe processes and workflow
- Re-scanning to verify that remediation actually occurred

### ***Step 3 – Report***

Regular reports are required for PCI compliance; these are submitted to the acquiring bank and global payment brands that you do business with. The PCI SSC is not responsible for PCI compliance. All merchants and processors must submit a quarterly scan report, which must be completed by a PCI SSC-approved ASV. Businesses with large flows must do an annual on-site assessment completed by a PCI SSC-approved QSA and submit the findings to each acquirer. Businesses with small transaction flows may be required to submit an annual Attestation within the [Self-Assessment Questionnaire](#). For more details, talk to your acquirer.

## **HIPPA Compliance** (Health Insurance Portability and Accountability Act of 1996) & **HITECH Act** (Health Information Technology for Economic and Clinical Health Act)

Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers.

AS also addresses the security and privacy of health data. The standards are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of [electronic data interchange](#) in the U.S. health care system.

HIPPA privacy regulations require health care organizations and their business associates develop and follow procedures that ensure the confidentiality and security of protected health information (PHI) when it is transferred, received, handled, or shared. This applies to all forms of PHI, including paper, oral, electronic, etc. Furthermore, only the minimum health information necessary to conduct business is to be used or shared. All covered entities are required to:

- Ensure the internal protection of individual health information and implement physical and administrative safeguards;
- Implement procedures that limit the use and disclosure of PHI to meet the "minimum necessary" standard;
- Develop mechanisms for the accounting and auditing of all disclosures made for purposes other than treatment, payment, or operations;
- Establish policies and procedures to allow individuals to amend their health information;
- Establish contracts and agreements with business associates that ensure the protection of PHI, which is shared or traded;
- Designate a privacy officer;
- Enforce penalties for misuse or inappropriate use of PHI; and
- Create and make available documentation regarding the compliance with all the requirements of the regulation.

The [Department of Health and Human Services](#) (HHS) has promulgated five rules regarding Administrative Simplification: the **Privacy Rule**, the **Transactions and Code Sets Rule**, the **Security Rule**, the **Unique Identifiers Rule**, and the **Enforcement Rule**.

### *Privacy Rule*

The Privacy Rule regulates the use and disclosure of Protected Health Information (PHI) held by "covered entities" (generally, health care clearinghouses, employer sponsored health plans, health insurers, and medical service providers that engage in certain transactions). By regulation, the Department of Health and Human Services extended the HIPAA privacy rule to independent contractors of covered entities who fit within the definition of "business associates". PHI is any information held by a covered entity which concerns health status, provision of health care, or payment for health care that can be linked to an individual. This is interpreted rather broadly and includes any part of an individual's medical record or payment history. Covered entities must disclose PHI to the individual within 30 days upon request. They also must disclose PHI when required to do so by law, such as reporting suspected child abuse to state child welfare agencies.

A covered entity may disclose PHI to facilitate treatment, payment, or health care operations, or if the covered entity has obtained authorization from the individual. However, when a covered entity discloses any PHI, it must make a reasonable effort to disclose only the minimum necessary information required to achieve its purpose.

The Privacy Rule gives individuals the right to request that a covered entity correct any inaccurate PHI. It also requires covered entities to take reasonable steps to ensure the confidentiality of communications with individuals. For example, an individual can ask to be called at his or her work number, instead of home or cell phone number.

The Privacy Rule requires covered entities to notify individuals of uses of their PHI. Covered entities must also keep track of disclosures of PHI and document privacy policies and procedures. They must appoint a Privacy Official and a contact person responsible for receiving complaints and train all members of their workforce in procedures regarding PHI.

An individual who believes that the Privacy Rule is not being upheld can file a complaint with the Department of Health and Human Services Office for Civil Rights (OCR). However, it is reported the OCR has a long backlog and ignores most complaints.

## ***Transactions and Code Sets Rule***

After July 1, 2005 medical providers filing electronically used HIPAA standards in order to be paid. On January 1, 2012 the newest version 5010 becomes effective; this allows for the larger field size of ICD-10-CM and other improvements.

### **Transactions types used to:**

- *EDI Health Care Claim Transaction set (837)* submit health care claim billing information and encounter information. It can be also be used for coordination of benefits (CoB) or monitoring industry segments.
- *EDI Retail Pharmacy Claim Transaction (NCPDP Telecommunications Standard version 5.1)* submit retail pharmacy claims. It can also be used for CoB or monitoring industry segments.
- *EDI Health Care Claim Payment/Advice Transaction Set (835)* make a payment, send an Explanation of Benefits (EOB), or send an Explanation of Payments (EOP).
- *EDI Benefit Enrollment and Maintenance Set (834)* to enroll members to a payer.
- *EDI Payroll Deducted and other group Premium Payment for Insurance Products (820)* make a premium payment for insurance or to order a financial institution to make a payment to a payee.
- *EDI Health Care Eligibility/Benefit Inquiry (270)* inquire about the health care benefits and eligibility associated with a subscriber or dependent.
- *EDI Health Care Eligibility/Benefit Response (271)* inquire about the health care benefits and eligibility associated with a subscriber or dependent.
- *EDI Health Care Claim Status Request (276)* request the status of a health care claim.
- *EDI Health Care Claim Status Notification (277)* respond to a health care claim status request.
- *EDI Health Care Service Review Information (278)* transmit health care service information for review.
- *EDI Functional Acknowledgement Transaction Set (997)* define the control structures for a set of acknowledgments.

## ***Security Rule***

The Final Rule on Security Standards took effect in April, 2003 with a compliance date in 2005 or 2006. The Security Rule complements the Privacy Rule. While the Privacy Rule pertains to all Protected Health Information (PHI) including paper and electronic, the Security Rule deals specifically with **Electronic Protected Health Information (EPHI)**. It lays out three types of security safeguards required for compliance: **administrative, physical, and technical**. For each of these types, the Rule identifies various security standards, and for each standard, it names both required and addressable implementation specifications. Required specifications must be adopted and administered as dictated by the Rule. Addressable specifications are more flexible. Individual covered entities can evaluate their own situation and determine the best way to implement addressable specifications. The standards and specifications are as follows:

**Administrative Safeguards** – policies and procedures designed to clearly show how the required entities will comply with the act. Covered entities must adopt a written set of privacy procedures and designate a privacy officer to be responsible for developing and implementing all required policies and procedures. The policies and procedures must reference management oversight and organizational buy-in to compliance with the documented security controls.

Procedures should clearly identify employees or classes of employees who will have access to electronic protected health information (EPHI). Access to EPHI must be restricted to only those employees who have a need for it to complete their job function. The procedures must address access authorization, establishment, modification, and termination. Entities must show that ongoing training is provided for employees performing health plan administrative functions.

Covered entities that out-source some of their business processes to a third party must ensure that their vendors also have a framework in place to comply with HIPAA requirements. Companies typically use contract clauses requiring the vendor to meet the same data protection requirements that apply to the covered entity. A contingency plan should be in place for responding to emergencies. Covered entities are responsible for backing up their data and having disaster recovery procedures in place. The plan should document data priority and failure analysis, testing activities, and change control procedures.

Internal audits play a key role in HIPAA compliance by reviewing operations with the goal of identifying potential security violations. Policies and procedures should specifically document the scope, frequency, and procedures of audits. Audits should be both routine and event-based. Procedures should document instructions for addressing and responding to security breaches that are identified either during the audit or the normal course of operations.

**Physical Safeguards** – controlling physical access to protect against inappropriate access to protected data. Controls must govern the introduction and removal of hardware/software from the network. Retired equipment must be disposed of properly to ensure that PHI is not compromised.

Access to equipment containing health information should be carefully controlled and monitored. Access to hardware and software must be limited to properly authorized individuals. Required access controls consist of facility security plans, maintenance records, and visitor sign-in and escorts.

Policies are required to address proper workstation use. Workstations should be removed from high traffic areas and monitor screens should not be in direct view of the public. If the covered entities utilize contractors or agents, they too must be fully trained on their physical access responsibilities.

**Technical Safeguards** – controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient. Information systems housing PHI must be protected from intrusion. When information flows over open networks, some form of encryption must be utilized. If closed systems/networks are utilized, existing access controls are considered sufficient and encryption is optional.

Each covered entity is responsible for ensuring that the data within its systems has not been changed or erased in an unauthorized manner. Data corroboration, including the use of check sum, double-keying, message authentication, and digital signature may be used to ensure data integrity. Covered entities must also authenticate entities with which they communicate. Authentication consists of corroborating that an entity is who it claims to be. Examples of corroboration include: password systems, two or three-way handshakes, telephone callback, and token systems.

Covered entities must make documentation of their HIPAA practices available to the government to determine compliance. In addition to policies and procedures and access records, information

technology documentation should also include a written record of all configuration settings on the components of the network because these components are complex, configurable, and always changing.

Documented risk analysis and risk management programs are required. Covered entities must carefully consider the risks of their operations as they implement systems to comply with the act. The requirement of risk analysis and risk management implies that the act's security requirements are a minimum standard and places responsibility on covered entities to take all reasonable precautions necessary to prevent PHI from being used for non-health purposes.

### ***Unique Identifiers Rule (National Provider Identifier)***

HIPAA covered entities such as providers completing electronic transactions, healthcare clearinghouses, and large health plans, must use only the National Provider Identifier (NPI) to identify covered healthcare providers in standard transactions. Use of electronic communications (e.g., physicians, hospitals, health insurance companies, etc) must use a single new NPI. The NPI replaces all other identifiers, is 10 digits (may be alphanumeric), and the last digit is a checksum. The NPI is unique, national, never re-used, and (except for institutions) a provider usually can only have one.

### ***Enforcement Rule***

In 2006, HHS issued the Final Rule regarding HIPAA enforcement, setting civil monetary penalties for violating HIPAA rules and establishing investigation and hearing procedures for HIPAA violations; its deterrent effects seem to be negligible with few prosecutions for violations.

### **HITECH Act (Health Information Technology for Economic and Clinical Health Act)**

Subtitle D of the HITECH Act, enacted as part of the American Recovery and Reinvestment Act of 2009, addresses the privacy and security concerns associated with the electronic transmission of health information.

This subtitle extends the complete Privacy and Security Provisions of HIPAA to business associates of covered entities. This includes the extension of newly updated civil and criminal penalties to business associates. These changes are also required to be included in any business associate agreements with covered entities. Significant changes are in breach notification and rules for accounting of disclosures of patient health information (limiting the timeframe for the accounting to three years instead of six).