



HIPAA Security Requirements

WHITE PAPER – July 2005

Notice: The contents of this briefing are not intended to serve as legal advice related to any individual situation. This material is made available from P4 Performance Management for informational purposes only and is provided with the understanding that P4 Performance Management is not providing legal advice. If legal advice is required, the services of a competent licensed attorney should be sought.

Security and Audit Requirements of the New Health Care Regulations

Each time a patient sees a doctor, is admitted to a hospital, goes to a pharmacist or sends a claim to a health plan, a record is made of their confidential health information. In the past, family doctors and other health care providers protected the confidentiality of those records by sealing them away in file cabinets and refusing to reveal them to anyone else.

Congress recognized the need for national patient record privacy standards in 1996 when they enacted the Health Insurance Portability and Accountability Act (HIPAA). The law included provisions to save money for the health care businesses by encouraging electronic transactions, but also required new safeguards to protect the security and confidentiality of that information. The law gave Congress until August 21, 1999, to pass comprehensive health privacy legislation. When Congress did not enact defining legislation, providing specifics for HIPAA compliance, the law required the Department of Health and Human Services (HHS) to craft such protections by regulation.

In November 1999, HHS published proposed regulations to guarantee patients new rights and protections against the misuse or disclosure of their health records. During an extended comment period, HHS received more than 52,000 communications from the public. In December 2000, HHS issued a final rule that made significant changes in order to address the issues that were raised. President George Bush and HHS Secretary Tommy Thompson allowed the rule to take effect on April 14, 2001. As required by the HIPAA law, most organizations have two years, until April 2003, to comply.

HIPAA regulations are forcing health record keepers to upgrade technical and administrative controls over the use, disclosure and transmission of patient information. Without a system that can

provide both security protections and thorough audit capabilities across an entire network, most organizations will be unable to come into compliance with the rules.

Organizations Affected by HIPAA

The privacy and security rules will apply directly to “covered entities” – including health care providers, plans, health care clearing houses, and those providers who conduct certain financial and administrative transactions (e.g. electronic billing, funds transfer) electronically. However, it will also affect companies and organizations not directly covered. That is a very big group because it includes all doctors, dentists, hospitals, clinics, pharmacies, nursing homes, laboratories, and health maintenance organizations, as well as the organizations that transfer health claims between providers and payers. Health care payers, insurers and support organizations, such as pharmacy benefit managers, will be covered.

Many corporations and federal, state and local government agencies that provide or pay for health care will also be covered.

If a person or organization transfers patient information to a business associate who provides services, then the business associate will be required by its contract to comply with many of the privacy requirements. When patient records are disclosed to lawyers, consultants, accountants, or to companies providing computer, administrative or financial services, many of the privacy obligations will flow with the records.

Information Covered by HIPAA

Under the privacy rule, protected health information includes virtually all data that can identify the patient. This might be address, social security number, driver’s license information, and even the patient’s employer’s name. Financial information about payments for health

care receives the same degree of privacy protection as health treatment data.

All health records are covered, regardless of the storage medium. Most HIPAA requirements apply to electronic transactions only, but the privacy rule applies broadly to all health information of a covered entity, including paper records.

Control over Health Information

Under the final rule, patients will have significant new rights to understand and control how their health information is used.

- **Patient education on privacy protections** – Providers and health plans will be required to give patients a clear written explanation of how the covered entity may use and disclose their health information.
- **Ensuring patient consent before information is released** – Patients will be able to see and get copies of their records, and request amendments. In addition, a history on non-routine disclosures must be made accessible to patients.
- **Receiving patient consent before information is released** – Health care providers who see patients will be required to obtain patient consent before sharing their information for treatment, payment and health care operations. In addition, separate patient authorization must be obtained for non-routine disclosures and most non-health care purposes. Patients will have their right to request restrictions on the uses and disclosures of their information.
- **Providing recourse in privacy protections are violated** – People will have the right to file a formal complaint with a covered provider or health plan, or with HHS, about violations of the provisions of this rule or the policies and procedures of the covered entity.

Another facet of use and disclosure is the minimum necessary rule. Most uses and disclosures must be limited to the minimum amount of information necessary to accomplish the intended purpose. The minimum necessary rule calls for reasonable efforts to restrict uses and disclosures. Current practices that involve the copying and disclosure of an entire patient record will no longer be permitted for most administrative or financial activities. However, the minimum necessary does not apply to treatment disclosures.

Administrative Requirements

A covered entity must (1) designate a privacy official; (2) provide staff training; (3) have a complaint process for individuals; and (4) document its policies and procedures.

In developing those policies and procedures, it will be essential to have a thorough understanding of the facilities' network and data facilities and the details of movement and location of the actual patient records. The policy must be adapted to the actual facility involved.

Today, many organizations do not understand the scope of the network assets. Tools, which automatically identify network assets and provide a real-time ontology (relationships between systems and users) can assist security managers in understanding their network assets and based on that define the required policies for that organization.

Security Requirements

The privacy rule requires covered entities to maintain appropriate administrative, technical and physical safeguards to protect the privacy of protected health information:

Administrative procedures to guard data integrity, confidentiality and availability:

These documented, formal practices manage the selection and execution of measures to protect data and the conduct of personnel. Specific requirements include chain of trust partner agreements, contingency planning for disasters, information access controls, personnel security, security incident procedures, security management (including risk analysis) and training.

Many of the detailed requirements reflect standard security practices. Contingency planning, formal mechanisms for processing records and information access controls are standard features. Personnel requirements include clearance, supervision, termination procedures, sanctions and training. Risk analysis will be important in making detailed security choices.

In order to perform risk analysis and security audits, the security manager must be able to:

- Identify activity on the network, normal or abnormal
- Identify areas of potential misuses
- Identify inappropriate transmission of information

P4 Performance Management's Gap Analysis enables companies to respond rapidly to protect their information assets through managed services that employ industry best practices with highly skilled and certified engineering resources. We help you protect the integrity of your company's network against abuses such as the improper transmittal of confidential patient information.

Physical safeguards to guard data integrity, confidentiality and availability:

These relate to the protection of physical computer systems, building and equipment from fire, other natural and environmental hazards and intrusion. Physical safeguards also cover the use

of locks, keys and administrative measures used to control access to computer systems and facilities. Specific requirements include media controls and physical access controls.

These requirements emphasize formal controls and documented policies. Each organization must have a security officer, and controls over hardware and software, including backup, storage and disposal. Physical access controls require formal plans controlling who may access the hardware and software elements of a system. Workstations must have physical access controls and policies for use (e.g. logging off rules for unattended terminals). Emergency and disaster plans are required, as is employee training in security awareness.

Technical security services to guard data integrity, confidentiality and availability:

These include processes to protect, control and monitor information access. Requirements include access controls, audit controls, authorization controls and entity authentication. Goals include limiting access to employees who have a need for information and controls to identify suspect activity.

P4 Performance Management can record and analyze all network activities to give the security officer the tools to protect mission critical information, such as intellectual property and confidential information, which are key to HIPAA compliance. It is also crucial to visually depict events in easily understood graphics which enables rapid response in the event of system misuse.

Technical security mechanisms:

These include processes to prevent unauthorized access to data transmitted over a communications network. Requirements include communications and network controls. The purpose is to protect communications during electronic transmission over open



networks and to prevent interception and use by third parties. Another goal is to prevent intruders from accessing systems through external communications points. For transmissions over open networks, encryption is required. For less open systems such as private lines and value-added networks, encryption is optional.

P4 Performance Management can forensically analyze all network collected traffic, as well as external data sources, such as log files, to drastically reduce the time required for investigations. If a situation should occur, sequence, view and playback events determine extent of the security problem under investigation and assess actual damage, whether direct or collateral. Then the data is output in an acceptable format for an evidentiary exhibit.

Accountability

In HIPAA, Congress provided serious penalties for the misuse of personal health information.

- **Civil penalties** – Health plans, providers and clearinghouses that violate these standards will be subject to civil liability. Civil monetary penalties are \$100 per violation, up to \$25,000 per person, per year for each requirement or prohibition violated.
- **Federal criminal penalties** – For knowingly violating patient privacy, criminal penalties are up to \$50,000 and one year in prison for obtaining or disclosing protected health information; up to \$100,000 and up to five years in prison for obtaining protected health information under “false pretenses”; and up to \$250,000 and up to 10 years in prison for obtaining or disclosing protected health information with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.

Conclusion

In order to comply with HIPAA regulations concerning privacy, security and to avoid costly litigation and fines, P4 Performance Management personnel and technologies are utilized for detection, abuse/misuse, risk assessment audits and forensics. With the serious monetary penalties allowed under HIPAA, investment in security services will more than justify the return on investment.

Contact Information

P4 Corporate Headquarters

MacGregor Park
130 Edinburgh Drive South, Suite 100
Cary, North Carolina 27511
Phone: 919-783-1500 or Fax: 919-783-1501