



HIPAA Compliance and Fleet Doctor Software Applications

Fleet Doctor Software Applications Do Not Impact HIPAA Compliance

The use of Fleet Doctor software applications will not have an impact on compliance with the Health Insurance Portability & Accountability Act (HIPAA) for covered entities. This is because the applications do not collect, house, or transmit any information regarding the content of print jobs, and thus have no way of accessing, housing, or transmitting electronic protected health information (ePHI) as defined by HIPAA.

However, you may need to obtain appropriate authorization according to your client's HIPAA compliance policies to gain access to a client site to install a Fleet Doctor Print Doctor Agent (PDA), or perform any other business, particularly if you are using a workstation or an area that has the capability of accessing ePHI. You should inquire about what authorization you will need, if any, beforehand.

Other aspects of your business, such as equipment placement, repair, maintenance, and/or disposal may require you to comply with additional sections of HIPAA regulations and will be discussed below.

How HIPAA Impacts Your Business

Organizations regulated by HIPAA need to ensure they are meeting the standards required by the Act when dealing with third party vendors. You should expect to be questioned about the installation, operation, and maintenance of any software or equipment that you are trying to place in an entity covered by HIPAA.

HIPAA includes a section, Title II, entitled Administrative Simplification which is broken down into the Security Rule, Privacy Rule, Identifiers, and Transactions & Code Sets. Of these, you should be aware of the Security Rule as a Fleet Doctor software vendor.

Security Rule

The Security Rule is composed of Administrative, Physical, and Technical Safeguards to ensure the security of protected health information that is housed or transmitted electronically. Your client's Security Officer will be primarily concerned with complying with the Security Rule when you approach them with Fleet Doctor software, or any new software or equipment.

1) Technical Safeguards

The Security Rule defines technical safeguards as "the technology and the policy and procedures for its use that protect electronic protected health information and control access to it."

With regards to technical safeguards, your client's Security Officer will be primarily concerned with the Transmission Security standard which requires covered entities to, "Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network."

The client will need to know that Fleet Doctor applications do not give you access to electronic protected health information. Fleet Doctor software applications do not collect any information regarding the content of print jobs, and thus have no way of accessing, housing, or transmitting electronic protected health information. Fleet Doctor software applications collect the device description, model, page counts, toner levels, serial number, LCD reading, device status, location, and asset number of printers, copiers, and multifunction devices. They do not collect any information regarding the content of print jobs.



2) Physical Safeguards

The Security Rule defines physical safeguards as “physical 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.” There are four physical safeguards that you should be aware of as discussed below.

i) Facility Access Controls

This standard requires covered entities to, “Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.”

If you are planning on visiting a client site to install a Fleet Doctor Print Doctor Agent, or perform any other business, you may need to receive authorization to access the facility and any specific areas of the facility that you need to be in. For example, you may need to wear a visitor badge or be accompanied by authorized personnel.

ii) Workstation Use

This standard requires covered entities to, “Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.”

This standard should not impact you other than to the extent that it may determine which workstations you can and cannot use for running and/or installing Fleet Doctor software. For example, you are unlikely to use a workstation that has access to ePHI.

iii) Workstation Security

This standard requires covered entities to, “Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.”

This standard should not impact you because you can run or install Fleet Doctor software on any Windows XP/2000 workstation, and it should not be one that has access to ePHI. In the unlikely circumstance that you must use a workstation with access to ePHI, you may be required to get authorization beforehand. Whenever possible, you should have the client operate the workstation to run and/or install the software.

iv) Device and Media Controls

This standard requires covered entities to, “Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information, into and out of a facility, and the movement of these items within the facility.”

This standard will not impact the use of Fleet Doctor applications, but may impact your business if you are an equipment vendor. Since many printing devices now have memory storage which is capable of retaining the content of print jobs, it is possible that printing devices will contain ePHI in their memory. Because of this, it is critical under HIPAA regulations that this ePHI be properly protected when the equipment is moved either within the facility or out of a facility.

The Device and Media Controls standard has required specifications for equipment disposal and re-use, which ensures that any ePHI will be removed and/or made inaccessible before the equipment is moved or removed from the facility. As an equipment vendor you may have responsibility in ensuring these specifications are met.



3) Administrative Safeguards

The Security Rule defines administrative safeguards as, “administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity’s workforce in relation to the protection of that information.”

Regardless of your business, if you are dealing with a HIPAA covered entity you may be impacted by administrative safeguards. As a third party vendor, you will be most impacted by the Business Associate Contracts standard which states that, “A covered entity, in accordance with § 164.306 [the Security Standards: General Rules], may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity’s behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a) [the Organizational Requirements] that the business associate will appropriately safeguard the information (Emphasis added).”

Your client may want you to become a Business Associate which will require you to have a written contract stating what satisfactory assurances you will make to safeguard any ePHI you come in contact with. This would apply, for example, if you have technicians that have access to device’s that may have memory storage containing ePHI. You also may be required to become a Business Associate under other sections of the law regarding non-electronic protected health information, for example if your technicians may come in contact with printed material.

HIPAA Overview

HIPAA is an acronym for the Health Insurance Portability & Accountability Act of 1996 (August 21), Public Law 104-191. It is also known as the Kennedy-Kassebaum Act. The Act is an amendment to the Internal Revenue Code of 1986.

The purpose of HIPAA is to improve efficiency in healthcare delivery by standardizing electronic data interchange, and protect the confidentiality and security of health data through setting and enforcing standards.

HIPAA includes a section, Title II, Administrative Simplification, which is composed of four parts which in themselves set out regulations and standards that must be followed by covered entities. The four parts are: Transactions and Code Sets, Unique Identifiers, Privacy, and Security.

Transactions and Code Sets

This rule adopts standards for eight electronic transactions and for code sets to be used in those transactions. It also contains requirements concerning the use of these standards by health plans, health care clearinghouses, and certain health care providers.

The use of these standard transactions and code sets will improve the Medicare and Medicaid programs and other Federal health programs and private health programs, and the effectiveness and efficiency of the health care industry in general, by simplifying the administration of the system and enabling the efficient electronic transmission of certain health information.

This rule covers the following types of electronic transactions: health claims or equivalent encounter information, health care payment and remittance advice, coordination of benefits, health claim status, enrollment and disenrollment in a health plan, eligibility for a health plan, health plan premium payments, referral certification and authorization.



Unique Identifiers

(1) National Provider Identifier Standard

This final rule establishes the standard for a unique health identifier for health care providers for use in the health care system and announces the adoption of the National Provider Identifier (NPI) as that standard. It also establishes the implementation specifications for obtaining and using the standard unique health identifier for health care providers. The implementation specifications set the requirements that must be met by “covered entities”: Health plans, health care clearinghouses, and those health care providers who transmit any health information in electronic form in connection with a transaction for which the Secretary has adopted a standard (known as “covered health care providers”). Covered entities must use the identifier in connection with standard transactions.

(2) National Employer Identifier

This final rule establishes a standard for a unique employer identifier and requirements concerning its use by health plans, health care clearinghouses, and health care providers. The health plans, health care clearinghouses, and health care providers must use the identifier, among other uses, in connection with certain electronic transactions.

Privacy Rule

This rule includes standards to protect the privacy of individually identifiable health information. The rules, which apply to health plans, health care clearinghouses, and certain health care providers, present standards with respect to the rights of individuals who are the subjects of this information, procedures for the exercise of those rights, and the authorized and required uses and disclosures of this information.

The use of these standards will improve the efficiency and effectiveness of public and private health programs and health care services by providing enhanced protections for individually identifiable health information. These protections will begin to address growing public concerns that advances in electronic technology and evolution in the health care industry are resulting, or may result, in a substantial erosion of the privacy surrounding individually identifiable health information maintained by health care providers, health plans and their administrative contractors.

Security Rule

This final rule adopts standards for the security of electronic protected health information to be implemented by health plans, health care clearinghouses, and certain health care providers. The use of the security standards will improve the Medicare and Medicaid programs, and other Federal health programs and private health programs, and the effectiveness and efficiency of the health care industry in general by establishing a level of protection for certain electronic health information.

The Covered Entities

Organizations that are regulated by HIPAA are called “covered entities”. The groups that are covered include health care providers, health plans, and health care clearinghouses. Any company that does business with a health care organization may also be affected, although not directly covered.

Protected Health Information

Protected health information is defined as “Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:

(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and



(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and: (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.”

Compliance Deadlines

As of October 2005, all compliance deadlines have passed with the exception of: Security Standards for small health plans (deadline: April 20, 2006), National Provider Identifier for all covered entities except small health plans (deadline: May 23, 2007), National Provider Identifier for small health plans (deadline: May 23, 2008).

Penalties for Violation

HIPAA has created severe penalties for non-compliance, including:

- Fines up to \$25K for multiple violations of the same standard in a calendar year
- Fines up to \$250K and/or imprisonment up to 10 years for knowing misuse of individually identifiable health information

For more Information

Office of Civil Rights: <http://www.hhs.gov/ocr/hipaa/>.

Sarbanes-Oxley Compliance and Implications for Fleet Doctor Software Applications

Fleet Doctor software is not intended to be used as part of an internal control structure as outlined in Section 404: Management Assessment of Internal Controls, but will not interfere with these controls.

Information Technology controls are an important part of complying with Sarbanes-Oxley. Under this Act, corporate executives become responsible for establishing, evaluating, and monitoring the effectiveness of internal control over financial reporting. There are IT systems in the market that are designed specifically for meeting these objectives. Fleet Doctor software is not designed as an IT control system, but will not interfere or put at risk other systems that are intended for that purpose.

A Fleet Doctor dealer may decide it is important to retain data collected with Fleet Doctor applications as part of Sarbanes-Oxley compliance if it is used as part of significant and routine financial transactions.

There are situations in which data collected with Fleet Doctor applications may be relevant to core financial processes within a business, primarily if the dealer is operating a cost per copy/page program using Fleet Doctor data as the source for invoicing. Fleet Doctor software collects page count MIB (Management Information Base) information from printers, copiers, fax machines, and multifunction devices. This allows dealers to charge their clients on a per page/copy basis over a specific billing period.

Fleet Doctor does not guarantee the accuracy of the information collected. Data is gathered directly from printer MIBs. Reasons for potential inaccuracy of page count information includes manual resetting of the page count meter by an onsite administrator, configuring a network timeout that is shorter than required to collect complete information, or



inaccuracy of the print device counter. Fleet Doctor applications make it easy to retain relevant data collected with and generated by the applications.

If a Fleet Doctor dealer decides that they do want to retain meter read data from the original Fleet Doctor application source, it is possible to retrieve this data in comma separated value format. From there the data can be easily transported to an electronic or other storage system.

Fleet Doctor uses an SQL database to retain all collected information until a user ceases to subscribe to the Fleet Doctor program, at which point their data will be removed. Meter read reports can be generated through the Fleet Doctor web interface, by selecting the Volume Report type from the Asset Reports selection under the Reporting menu. By choosing to email these reports, the recipient will receive a copy in comma separated value format which can then be transferred to a storage system. It is the primary responsibility of the Fleet Doctor user to ensure specific data is backed up to prevent loss.

Sarbanes-Oxley Overview

The Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (July 30, 2002), is a United States federal law also known as the Public Company Accounting Reform and Investor Protection Act of 2002. It is also commonly known as SOX or SarbOx.

The Act ensured the creation of public company accounting oversight board, auditor independence, corporate responsibility, and enhanced financial disclosures.

As referenced previously, Section 404 of the Act is as follows:

SEC. 404. MANAGEMENT ASSESSMENT OF INTERNAL CONTROLS.

(a) **RULES REQUIRED-** The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) to contain an internal control report, which shall--

(1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and

(2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

(b) **INTERNAL CONTROL EVALUATION AND REPORTING-** With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.

For more information:

Wikipedia: http://en.wikipedia.org/wiki/Sarbanes-Oxley_Act

Legal Archiver: <http://www.legalarchiver.org/soa.htm>

Public Company Accounting Oversight Board Official Website: <http://www.pcaobus.org/>