



HIPAA: The Role of PatientTrak.net in Supporting Compliance

The purpose of this document is to describe the methods by which PatientTrak.net addresses the requirements of the HIPAA Security Rule, as pertaining to the storing, maintaining, and transmission of electronic health information.

While PatientTrak.net provides methods to address the requirements of the HIPAA Security Rule, it is the responsibility of each business entity to enforce the entity's documented HIPAA security policies and procedures.

HIPAA: The Role of PatientTrak.net in Supporting Compliance

NOTICES

Copyright

© PatientTrak.net, 2009, all rights reserved

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written consent of PatientTrak.net.

Trademarks

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written consent of PatientTrak.net.

PatientTrak.net may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from PatientTrak.net, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

2009 PatientTrak.net. All rights reserved.

Disclaimer

The information contained in this document represents the current release of PatientTrak.net and the current interpretations of HIPAA at the time of publication. PatientTrak.net cannot guarantee the accuracy of any information that is based on the interpretations of HIPAA after the date of publication.

This document is for informational purposes only. PatientTrak.net makes no warranties, express or implied, in this document.

This paper is not intended as legal or compliance advice. Speak to a HIPAA compliance expert about how HIPAA affects your business and what steps you need to take to comply.

HIPAA: The Role of PatientTrak.net in Supporting Compliance

Contents

COPYRIGHT2
 TRADEMARKS2
CONTENTS3
HIPAA SECURITY RULE OVERVIEW4
 WHAT IS THE HIPAA SECURITY RULE?.....4
 IMPLEMENTING THE HIPAA SECURITY RULE.....4
PATIENTTRAK.NET AND SECURITY RULE REQUIREMENTS6
 ACCESS CONTROL & AUTHENTICATION6
 I) *Unique User Identification Requirements - HIPAA*6
 I) *Unique User Identification Requirements – PatientTrak.net*7
 II) *Emergency Access Procedure Requirements - HIPAA*7
 II) *Emergency Access Procedure Requirements - PatientTrak.net*.....7
 III) *Automatic Logoff - HIPAA*.....8
 III) *Automatic Logoff - PatientTrak.net*8
 IV) *Encryption and Decryption Requirements - HIPAA*8
 IV) *Encryption and Decryption Requirements - PatientTrak.net*.....9
 AUDIT CONTROLS & INTEGRITY CONTROLS9
 V) *Audit Control Requirements - HIPAA*.....9
 V) *Audit Control Requirements - PatientTrak.net*.....9
 VI) *Integrity Control Requirements - HIPAA*.....10
 VI) *Integrity Control Requirements - PatientTrak.net*10
SUMMARY11

HIPAA: The Role of PatientTrak.net in Supporting Compliance

HIPAA Security Rule Overview

This section provides an overview of the HIPAA Security Rule. A detailed review of the Security Rule will be presented in the next section. The next section will also detail how PatientTrak.net meets or exceeds the minimum security requirements as set forth by the Final Security Rule.

What is the HIPAA Security Rule?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a comprehensive piece of legislation, which among other things includes the HIPAA Security Rule. The HIPAA Security Rule provides guidelines for ensuring privacy and confidentiality in storing, maintaining, or transmitting health information. The final Security Rule was released by the Department of Health and Human Services on April 20, 2003. The compliance date for security is April 21, 2005.

The Final Security Rule covers all health care information electronically maintained or transmitted, either internally or externally. Covered entities include health plans, health care clearinghouses, and health care providers, among other healthcare-related organizations. The Security Rule describes the security requirements for health information that must be in effect to be in compliance with the Administrative Simplification portion of HIPAA Title II.

Implementing the HIPAA Security Rule

Each business entity can determine what techniques and controls should be implemented to provide appropriate and adequate protection of electronic information. The controls to be implemented should be determined by the size of the organization, as well as the nature of the electronic information being stored, maintained, or transmitted. Covered entities must ensure the confidentiality and integrity of all electronic health information, must protect against any reasonably anticipated threats or hazards to the data, must protect against any reasonably anticipated uses or disclosures of the data, and must ensure compliance by all staff through documented policies and procedures.

The following security terms and definitions are used in implementing policies and procedures to safeguard health information. These terms will be referenced throughout the remainder of this document.

- “Authentication” is the means by which a user proves their identity.
- “Access Control” is providing restrictions on users to read, write, or edit health information in order to protect against unauthorized manipulation of the data.

HIPAA: The Role of PatientTrak.net in Supporting Compliance

- “Confidentiality” concerns the protection of data from unauthorized disclosure to non-authorized internal or external parties.
- “Integrity” means that the data is accurate and has not been altered or deleted by an unauthorized user.
- “Availability” means that the health information is readily accessible by an authorized user on demand.
- “Encryption” is the means by which data is translated to a form that is unreadable by unauthorized users.
- “Physical Safeguards” are physical policies and procedures used to ensure that the equipment used to store health information is protected from reasonably anticipated physical hazards.
- “Role-based Security” is the recommended means of allowing access to data by authorized users while disallowing access to data by unauthorized users through the use of Roles assigned to groups of users, which determine the minimum requirements for each group of users to complete their jobs.

HIPAA: The Role of PatientTrak.net in Supporting Compliance

PatientTrak.net and Security Rule Requirements

This section has a dual purpose. The first purpose of this section is to provide the detailed HIPAA security requirements that must be implemented by all covered entities. The second purpose of this section is to provide the methods by which PatientTrak.net meets or exceeds these security requirements. To provide a more readable format, this section is formatted such that each detailed HIPAA security requirement will be followed immediately by a description of PatientTrak.net's method of meeting or exceeding each security requirement.

There are multiple sections within the HIPAA Security Rule. The Technical Safeguards section provides standards on implementing policies and procedures to protect and control access to electronic health information. The Technical Safeguards section of the HIPAA Security Rule includes standards on:

- Access Control
- Audit Controls
- Person or Entity Authentication
- Transmission Integrity & Security

This document has combined the elements of the Technical Safeguards section in two sections. The first section reviews Access Control and Authentication. The second section reviews Audit Controls and Data Integrity.

The standards provided by HIPAA are either Required or Addressable by all covered entities. The term Addressable means that the standard is not currently required, but is recommended by HIPAA and should be given consideration either currently or during future projects or planning.

Access Control & Authentication

Access Control, or authorization, refers to the presence of restrictions on a user's ability to access resources or information.

I) Unique User Identification Requirements - HIPAA

The HIPAA Final Security Rule requires that a User ID and password system be used by all covered entities in order to gain access to all electronic health information.

Furthermore, the Security Rule states that each user should only be granted adequate access to complete the required tasks. Such role-based security methods provide for additional security by allowing only authorized personnel to perform certain functions while working with covered electronic health information.

HIPAA: The Role of PatientTrak.net in Supporting Compliance

I) Unique User Identification Requirements – PatientTrak.net

In order to gain access to PatientTrak.net, each user must provide a unique User ID and password. The User ID is used to authenticate each unique user of the system. Once logged onto the system, each transaction accessed or deleted by the user is tracked, providing for an audit-trail of each user's activities. (See also section V on Audit Controls)

PatientTrak.net also utilizes role-based security to determine what functions a user is allowed to perform while logged in to PatientTrak.net. Examples of pre-defined roles include read-only access, standard user access, and administrative privileges.

II) Emergency Access Procedure Requirements - HIPAA

The HIPAA Final Security Rule requires that covered entities define and document a procedure that will be used if access to electronic health information is restricted temporarily by emergency, natural disaster, or other un-planned event. It is the responsibility of each covered entity to ensure that the plan has been clearly communicated to all related parties.

II) Emergency Access Procedure Requirements - PatientTrak.net

The primary functions of PatientTrak.net are to capture the time and area to which a patient has been admitted and to track the patient's movements and final discharge from the facility. As additional functions, limited details may be entered regarding the patient including the status of patient activities; however, the primary functions remain the monitoring of the patient's time and location while within the facility. The benefits of tracking this information electronically include statistical reporting on patient throughput time, high-efficiency personnel, and peak time facility or resource usage.

Many covered entities that have begun using PatientTrak.net had previously tracked patient flow throughout the department via dry-erase boards. PatientTrak.net recommends that PatientTrak.net be used in a similar fashion to a dry-erase board. PatientTrak.net is an electronic computer system that maintains access to health information via an Internet connection or through the organization's servers and network. Due to the fact that PatientTrak.net is an electronic computer system and no computer system can guarantee one hundred percent reliability in the case of a natural disaster or other un-planned event, PatientTrak.net encourages each covered entity to maintain a manual system as an emergency access procedure for tracking patient flow through the facility. This manual system should be documented and each covered entity should ensure that all users of PatientTrak.net are made aware of the emergency access procedures.

HIPAA: The Role of PatientTrak.net in Supporting Compliance

III) Automatic Logoff - HIPAA

The HIPAA Final Security Rule recommends, but does not require, that all systems used to store electronic health information have an automatic logoff feature after a pre-defined period of inactivity. This is an addressable standard that is not required by the HIPAA Final Security Rule. The Security Rule does not specify the period of time at which the system should automatically logoff the user. Instead, it allows for each covered entity to determine the implementation of automatic logoff based on the size of the covered entity and the nature of the electronic health information being stored and maintained by each system.

III) Automatic Logoff - PatientTrak.net

PatientTrak.net utilizes a standard Microsoft Internet Explorer web-browser to display the electronic health information that is stored and maintained by the system. Because the automatic logoff standard is an addressable standard and not a required standard, it is up to each covered entity to determine the amount of time that must elapse before the computer session expires.

PatientTrak.net was previously designed to include an automatic logoff feature, but after receiving a consensus of feedback from the existing client base of PatientTrak.net, it was decided to remove this feature. The primary reason cited for requesting the removal of the automatic logoff feature from the standard product was due to the loss in productivity from requiring logging in each time the system is accessed, which is quite frequently. As such, it was determined that the benefits of the automatic logoff feature did not outweigh the benefits of having a system that was always accessible to the user regardless of the amount of time elapsed between each use of the system.

PatientTrak.net users may implement a screensaver with a password on each PC using the PatientTrak.net system, in order to allow control over the automatic "logout" at the PC level.

At the request of any covered entity, PatientTrak.net will attempt to provide a solution that includes the automatic logoff feature.

IV) Encryption and Decryption Requirements - HIPAA

The HIPAA Final Security Rule recommends, but does not require, that all electronic health information that is stored or maintained be encrypted during transmission. This is an addressable standard that is not required by the HIPAA Final Security Rule. Covered transmission includes sending the data internally (for example, from a server to a workstation), or externally (for example, from a server to a third-party outside of the covered entities protected network).

HIPAA: The Role of PatientTrak.net in Supporting Compliance

IV) Encryption and Decryption Requirements - PatientTrak.net

All data transmitted by PatientTrak.net is fully encrypted when transmitted externally via the Internet. The encryption techniques utilized are similar to those methods used to transmit banking data or social security information. In the transmission of all data within the system, PatientTrak.net utilizes full 128-bit SSL Secured encryption from Comodo Class 3 Security Services.

Audit Controls & Integrity Controls

V) Audit Control Requirements - HIPAA

The HIPAA Final Security Rule requires that mechanisms are in place to record access to electronic health information. These mechanisms may include logging of user access attempts to the system as well as logging of user activity once in the system. Each covered entity will have the ability to determine what activities are monitored and at what level of detail the audit trails are maintained. However, the Security Rule does not require that detailed audit trails are maintained.

The Security Rule also requires that all audit control mechanisms are documented. The documentation of audit controls should include information such as what audit data is being maintained, how long the audit data is to be maintained, where the audit data is stored, and which users are allowed to access the audit data.

V) Audit Control Requirements - PatientTrak.net

PatientTrak.net runs on the Microsoft Windows 2003 Server operating system and the PatientTrak.net database engine is powered by Microsoft SQL Server. These systems each contain extensive transaction logging systems that monitor both successful and unsuccessful attempts at accessing the systems currently running within its framework. Windows 2003 Server includes the monitoring of account management events, logon events, database object access events, and system events. Microsoft SQL Server provides for detailed user access transaction logging as well as database-level security to ensure that each user is only allowed to perform those functions that have been assigned to the user.

PatientTrak.net maintains a detailed audit trail within the database of each instance of a user login, and each instance of access to a patient record. PatientTrak.net builds detailed audit trail records that indicate the user that accessed the record and the date and the time of the access. PatientTrak.net maintains the audit trails and makes the data available to the covered entity on-demand via an administrator-protected utility.

HIPAA: The Role of PatientTrak.net in Supporting Compliance

VI) Integrity Control Requirements - HIPAA

The HIPAA Final Security Rule recommends, but does not require, that adequate integrity controls are implemented in order to ensure that electronic health information has not been altered or deleted by an unauthorized user. These controls include both authentication methods to ensure that only authorized users are able to access the data as well as system controls to ensure that the electronic health information is accurate and accessible as required by authorized users.

VI) Integrity Control Requirements - PatientTrak.net

PatientTrak.net utilizes several methods to provide for the requirements of user authentication. These methods include unique user identification and password required to access PatientTrak.net, SQL Server-based authentication at the database level, and user access audit trails within the database to track and maintain a history of data access by authorized users. All of these methods assist in ensuring the complete integrity of the PatientTrak.net database.

SQL Server provides several methods for ensuring that the data stored within each SQL Server database is accurate and available for on-demand access by authorized users. SQL Server database tools available to ensure that data integrity is maintained include transactions, locks, and lock escalation.

HIPAA: The Role of PatientTrak.net in Supporting Compliance

Summary

Covered business entities must comply with the HIPAA Final Security Rule by April 21, 2005. Covered entities include health plans, health care clearinghouses, and health care providers. The Final Security Rule covers all health care information electronically stored or maintained in an electronic transmission, either internally or externally.

Each business entity can determine what techniques and controls should be implemented to provide appropriate and adequate protection of electronic information. This determination should be based on the size of the business and the nature of the electronic information being stored, maintained, or transmitted. Covered entities have several responsibilities relating to electronic health information including ensuring the confidentiality and integrity of all electronic health information, protecting against any reasonably anticipated threats or hazards to the data, protecting against any reasonably anticipated uses or disclosures of the data, and ensuring compliance by all staff through documented policies and procedures.

PatientTrak.net is an easy-to-use web-based patient tracking system that can be utilized to improve departmental or organization-wide patient flow and efficiency.

PatientTrak.net provides management with the information necessary to accurately compile meaningful statistical patient flow reporting and analysis.

PatientTrak.net utilizes a wide range of tools and methods for assisting business entities with complying with the HIPAA Final Security Rule. Within the application, PatientTrak.net utilizes User Logins and Passwords, Role-based security, secure data encryption during all data transmission, and extensive audit trails of user activities. Built on Microsoft technologies including Windows 2003 Server, SQL Server, and Internet Information Server, PatientTrak.net leverages the security tools and techniques of the world's premier software company to provide for a secure environment.

PatientTrak.net can be utilized to assist a covered entity with complying with the HIPAA Final Security Rule. PatientTrak.net can be tailored to meet any additional requirements requested by a covered entity utilizing PatientTrak.net. PatientTrak.net will continue to monitor any future changes or additions to the HIPAA Security Rule to ensure that it meets or exceeds the minimum-security requirements set forth within the HIPAA Security Rule or any future changes or amendments.