McKESSON
Empowering Healthcare

Performance Analytics

Powered by Horizon Business Insight

Security and Privacy Guide

Release 14.0
April 2009

Publication date

April 2009
Produced in Ireland

Product

Horizon Performance Manager Release 14.0

Corporate address

McKesson Corporation
5995 Windward Parkway
Alpharetta, GA 30005
404-338-6000

Reader comments

Comments or suggestions regarding this publication are welcome and should be sent to the following address:

McKesson Corporation
Horizon Business Insight Documentation Team
380 Russell Street
Hadley, MA 01035

Table of Contents

Document Information i
About This Document v

Chapter 1 - Security Standards **1-1**
Administrative Safeguards 1-2
Security Management Process 1-3
Workforce Security 1-4
Information Access Management 1-5
Security Awareness and Training 1-6
Contingency Plan 1-7
Physical Safeguards 1-8
Device and Media Controls 1-9
Technical Safeguards 1-10
Access Control 1-11
Audit Controls 1-13
Integrity 1-14
Person or Entity Authentication 1-15
Transmission Security 1-16

Chapter 2 - Privacy Standards **2-1**
Uses and Disclosures of Protected Health Information: General Rules 2-2
Uses and Disclosures: Consent and Authorizations 2-3
Use and Disclosures for Facility Directories/Clergy Lists 2-4
Other Requirements Relating to Uses and Disclosures of Protected Health Information 2-5
Confidential Communications Requirements 2-6

About This Document

This section provides information to help you understand the *Security and Privacy Guide* and how to most effectively use it.

Purpose

This document is intended to help you use Horizon Business Insight™ within the framework and guidelines of HIPAA standards. It is not intended to address operating system security issues or to recommend network configurations that transcend Horizon Business Insight.

Audience

This document is intended for HIPAA privacy and security officers, decision support coordinators, system managers and database administrators.

Organization

This document contains two major chapters: Security Standards and Privacy Standards. Each section in the chapters references and summarizes a standard and its implementation specifications, lists relevant activities in Horizon Business Insight, and points you to the Horizon Business Insight information that describes how to accomplish the tasks and activities. Horizon Business Insight information can be:

- training classes
- documentation

Referenced Documentation

The following Horizon Performance Manager guides and manuals are referenced in this document.

- *Horizon Performance Manager User's Guide*
- *Horizon Business Insight Installation Guide*
- *Horizon Business Insight Upgrade Guide*
- *Other McKesson Products Software Setup*
- *Horizon Modules*

Also, the following volumes of the *Federal Register* are referenced:

- Vol. 65, No. 250, *Federal Register* 45 CFR Parts 160 and 164, Standards for Privacy of Individually Identifiable Health Information; Final Rule, published on Thursday, December 28, 2000.

- Vol. 67, No. 157, *Federal Register* 45 CFR Parts 160 and 164, Standards for Privacy of Individually Identifiable Health Information; Final Rule, published on Wednesday, August 14, 2002.
- Vol. 68, No. 34, *Federal Register* 45 CFR Parts 160, 162 and 164, Security Standards; Final Rule, published on Thursday, February 20, 2003.

Chapter 1 - Security Standards

This chapter refers to Vol. 68, No. 34, *Federal Register* 45 CFR Parts 160, 162 and 164, Security Standards; Final Rule, published on Thursday, February 20, 2003.

In This Chapter

This chapter contains the following topics:

Topic	See Page
Administrative Safeguards	1-2
Physical Safeguards	1-8
Technical Safeguards	1-10

Administrative Safeguards

In This Section

The following standards are discussed in this section:

Topic	See Page
Security Management Process	1-3
Workforce Security	1-4
Information Access Management	1-5
Security Awareness and Training	1-6
Contingency Plan	1-7

Security Management Process

Standard

Section **164.308(a)(1)(i)**, *Security management process*, requires each entity to implement policies and procedures to prevent, detect, contain, and correct security violations.

The following implementation specification is relevant to Horizon Business Insight:

- **164.308(a)(1)(ii)(D)** -- Information system activity review (Required)

Activities Related to Horizon Business Insight

This standard requires your organization to put in place formal procedures to protect data. One of the technical safeguards used to support these procedures is Audit Controls (section **164.312(b)**). See “Audit Controls” on page 1-13 of this document.

Workforce Security

Standard

Section **164.308(a)(3)(i)**, *Workforce security*, requires each entity to implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information. Additionally, the entity must prevent those workforce members who do not have access to electronic protected health information from obtaining access.

The following implementation specifications are relevant to Horizon Business Insight:

- **164.308(a)(3)(ii)(B)** -- Workforce clearance procedures (Addressable)
- **164.308(a)(3)(ii)(C)** -- Termination procedures (Addressable)

Activities Related to Horizon Business Insight

The following Horizon Business Insight functionality supports this standard:

- A current record of users and their privileges to sites and access to objects can be maintained utilizing the access reports in the Administrator. These reports allow you to report by site, group, user or object. For example, to create a report that shows the site privileges and object access by users, select Administrator>Users>**Access Reporting**.
- User accounts can be deleted in the Horizon Business Insight Administrator (Administrator>Users>**Delete**).

  Caution: Deleting a user account in the Administrator does not delete the account from the operating system or domain.

- Site privileges can be removed from a user's account (Administrator>Users> click **Privileges** for a specific user).

Horizon Business Insight Information

- *Horizon Business Insight User's Guide*
  - refer to the chapter entitled, "Using the Administrator" for information on the Access Reports.
  - refer to the chapter entitled, "Using the Administrator" for information on users accounts and privileges.
- Administrator online help

Information Access Management

Standard

Section **164.308(a)(4)(i)**, *Information access management*, requires each entity to implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements.

The following implementation specifications are relevant to Horizon Business Insight:

- **164.308(a)(4)(ii)(B)** -- Access authorization (Addressable)
- **164.308(a)(4)(ii)(C)** -- Access establishment and modification (Addressable)

Activities Related to Horizon Business Insight

Your organization may create policies and procedures to address this standard. Though the creation of these policies and procedures is not directly related to Horizon Business Insight, their implementation is directly related.

For information related to the implementation of Access Control see “Access Control” on page 1-11 of this document.

Security Awareness and Training

Standard

Section **164.308(a)(5)(i)**, *Security awareness and training*, requires each entity to implement a security awareness and training program for all members of its workforce (including management).

The following implementation specifications are relevant to Horizon Business Insight:

- **164.308(a)(5)(ii)(C)** -- Log-in monitoring (Addressable)
- **164.308(a)(5)(ii)(D)** -- Password management (Addressable)

Activities Related to Horizon Business Insight

Horizon Business Insight security is closely related to the operating system security. Since both log-in monitoring and password management features are available in the operating system, they are also available to Horizon Business Insight.

Other Information

See Microsoft's *Active Directory for Users and Computers* (Windows 2003) for more information on security.

Contingency Plan

Standard

Section **164.308(a)(7)(i)**, *Contingency plan*, requires each entity to establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

The following implementation specifications are relevant to Horizon Business Insight:

- **164.308(a)(7)(ii)(A)** -- Data backup plan (Required)
- **164.308(a)(7)(ii)(B)** -- Disaster recovery plan (Required)

Activities Related to Horizon Business Insight

You may want to address the following topics in your contingency plan:

- creating a data backup / recovery plan
- backing up the Horizon Business Insight server regularly
- keeping installation media and documentation

Horizon Business Insight Information

All installation/upgrade documentation can be found on the Horizon Business Insight Documentation CD.

Backup and restore guidelines can be found in the appendix of the *Horizon Business Insight Installation Guide*.

Other Information

The following Microsoft resources may be helpful:

- Windows 2003 Server security patches
- Windows 2003 Server security best practices
- SQL Server 2003 best practices

Note: McKesson cannot fully test and certify all Microsoft patches and recommendations as soon as they are released.

Physical Safeguards

In This Section

The following standard is discussed in this section:

Topic	See Page
Device and Media Controls	1-9

Device and Media Controls

Standard

Section **164.310(d)(1)**, *Device and media controls*, requires that each entity 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 movement of these items within the facility.

The following implementation specifications are relevant to Horizon Business Insight:

- **164.310(d)(2)(i)** -- Disposal (Required)
- **164.310(d)(2)(iv)** -- Data backup and storage (Required)

Activities Related to Horizon Business Insight

Refer to your operating system, SQL or third-party backup software documentation for backing up operating system files and SQL database files.

All installation/upgrade documentation can be found on the Horizon Business Insight Documentation CD.

Backup and restore guidelines can be found in the appendix of the *Horizon Business Insight Installation Guide*.

Horizon Business Insight Information

Backup and restore guidelines can be found in the appendix of the *Horizon Business Insight Installation Guide*.

Technical Safeguards

In This Section

The following standards are discussed in this section:

Topic	See Page
Access Control	1-11
Audit Controls	1-13
Integrity	1-14
Person or Entity Authentication	1-15
Transmission Security	1-16

Access Control

Standard

Section **164.312(a)(1)**, *Access control*, requires the implementation of technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights.

The following implementation specifications are relevant to Horizon Business Insight:

- **164.312(a)(2)(i)** -- Unique user identification (Required)
- **164.312(a)(2)(iii)** -- Automatic logoff (Addressable)
- **164.312(a)(2)(iv)** -- Encryption and decryption (Addressable)

Activities Related to Horizon Business Insight

The following Horizon Business Insight functionality supports this standard:

- Horizon Business Insight utilizes unique user IDs and passwords.
  - Passwords are managed by the Windows 2003 operating system; therefore, any password management functionality available in the operating system, such as setting password expiration and minimum password length, is available to Horizon Business Insight passwords.

  Note: User privileges to sites and access to objects can be identified by creating Access Reports in the Administrator.

- To prevent unauthorized access to workstations, you may want to activate a password-protected screen saver. Microsoft Windows screen savers can be activated on each workstation, or you could adopt a centrally-managed solution such as NetOFF™ from Citadel Security Software, Inc.

  Caution: Individual users have the ability to deactivate a password-protected Microsoft Windows screen saver.

- Horizon Business Insight's automatic logout functionality terminates the current browser session after a period of inactivity in the Horizon Business Insight website. Users are prompted for domain, user name and password when attempting to log back into the site. In addition, identifying information must be entered when a menu option that opens another Horizon Business Insight site is selected.

  The automatic logout functionality applies to all of the Horizon Business Insight websites. The default timeout periods for the Horizon Business Insight websites are as follows:

  - Subset Editor site 20 minutes
  - All other HBI sites 60 minutes

- Horizon Business Insight does not encrypt electronic protected health information. It is your responsibility to deploy the server in a secure environment coupled with the access control features provided with Horizon Business Insight.

Horizon Business Insight Information

- *Horizon Business Insight User's Guide*
  - refer to the chapter entitled, "Using the Administrator" for information on assigning passwords to users.
  - refer to "Appendix A - Security" for a description of password maintenance functionality.
- Administrator online help
- Horizon Business Insight Technical Training class

Other Information

Horizon Business Insight security is closely related to the operating system security. See Microsoft's Active Directory for Users and Computers (Windows 2003) for more information.

Audit Controls

Standard

Section **164.312(b)**, *Audit controls*, requires each entity to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. This is required.

Activities Related to Horizon Business Insight

The following Horizon Business Insight functionality supports this standard:

- Access Reports can be created to determine which users have privileges to which Horizon Business Insight sites and objects. For example, click Administrator>Users>**Access Reporting** to create a report organized by user.
- The **Horizon Business Insight Utilization Report** can be used to review user and group access to highlights, reports, resources and scorecards from the Viewer site.
- The **Horizon Business insight Activity Report** can be used to review user administrative activities performed in the Administrator, Highlight Editor, Scorecard Editor and Subset Editor sites.

Horizon Business Insight Information

- *Horizon Business Insight User's Guide*
  - refer to the chapter entitled, "Using the Administrator" for information on the Access Reports.
- Administrator online help
- Horizon Business Insight Technical Training class

Integrity

Standard

Section **164.312(c)(1)**, *Integrity*, requires each entity to implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

The following implementation specification is relevant to Horizon Business Insight:

- **164.312(c)(2)** -- Mechanism to authenticate electronic protected health information (Addressable)

Activities Related to Horizon Business Insight

The following Horizon Business Insight functionality supports this standard:

- Access Reporting can be used to review who has privileges to the Highlight Editor and Subset Editor -- those are the sites that can modify data.
- The Administrator can be used to limit the number of users who have privileges to the Highlight Editor and Subset Editor (Administrator> Users>click **Privileges** for a specific user).

Horizon Business Insight Information

- *Horizon Business Insight User's Guide*
  - refer to the chapter entitled, "Using the Administrator" for information on granting privileges.
- Administrator online help
- Horizon Business Insight Technical Training class

Person or Entity Authentication

Standard

Section **164.312(d)**, *Person or entity authentication*, requires the implementation of procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. This is required.

Activities Related to Horizon Business Insight

- Horizon Business Insight utilizes unique IDs and passwords to support entity authentication.
  - Passwords are managed by the Windows 2003 operating system; therefore, any password management functionality available in the operating system, such as setting password expiration and minimum password length, is available to Horizon Business Insight passwords.
  - Horizon Business Insight's automatic logout functionality terminates the current browser session after a period of inactivity in any of the Horizon Business Insight websites. Users are prompted for domain, user name and password when attempting to log back into the site. In addition, identifying information must be entered when a menu option that opens another Horizon Business Insight site is selected. The automatic logout functionality applies to all of the Horizon Business Insight websites. The default timeout periods for the Horizon Business Insight websites are as follows:
    - Subset Editor site 20 minutes
    - All other HBI sites 60 minutes

Horizon Business Insight Information

- *Horizon Business Insight User's Guide*
  - refer to the chapter entitled, "Using the Administrator" for information about changing user passwords.
  - refer to "Appendix A - Security" for a description of password maintenance functionality.
- Administrator online help

Other Information

Horizon Business Insight security is closely related to the operating system security. See Microsoft's *Active Directory for Users and Computers* (Windows 2003) for more information on security.

Transmission Security

Standard

Section **164.312(e)(1)**, *Transmission security*, requires that each entity implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

The following implementation specification is relevant to Horizon Business Insight:

- **164.312(e)(2)(i)** -- Integrity controls (Addressable)

Activities Related to Horizon Business Insight

- Consider using McKesson's CareBridge™, which offers more security than a modem, to help you control and monitor access to your system and information.

Horizon Business Insight Information

Refer to the *Horizon Business Insight Installation Guide* for details about how the Horizon Business Insight server should be installed and configured.

Chapter 2 - Privacy Standards

This chapter refers to the following documents:

- Vol. 67, No. 157, Federal Register 45 CFR Parts 160 and 164, Standards for Privacy of Individually Identifiable Health Information; Final Rule, published on Wednesday, August 14, 2002.
- Vol. 65, No. 250, Federal Register 45 CFR Parts 160 and 164, Standards for Privacy of Individually Identifiable Health Information; Final Rule, published on Thursday, December 28, 2000.

In This Chapter

This chapter contains the following topics:

Topic	See Page
Uses and Disclosures of Protected Health Information: General Rules	2-2
Uses and Disclosures: Consent and Authorizations	2-3
Use and Disclosures for Facility Directories/Clergy Lists	2-4
Other Requirements Relating to Uses and Disclosures of Protected Health Information	2-5
Confidential Communications Requirements	2-6

Uses and Disclosures of Protected Health Information: General Rules

Standards

Section **164.502(b)** states that a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

Sections **164.514(d)(2)(i)(A)** and **164.514(d)(2)(i)(B)** state that a covered entity must identify those persons or classes of persons, as appropriate, in its workforce who need access to protected health information to carry out their duties, and then identify the category or categories of protected health information to which access is needed and any conditions appropriate to such access.

This idea is also reflected in the preamble of the final privacy rule (page 82544), which states, "A covered entity must implement policies and procedures to identify the persons or classes of persons in the entity's workforce who need access to protected health information to carry out their duties, the category or categories of protected health information to which such persons or classes need access, and the conditions, as appropriate, that would apply to such access. Covered entities must also implement policies and procedures to limit access to only the identified persons, and only to the identified protected health information."

Activities Related to Horizon Business Insight

Horizon Business Insight can be used to control the distribution of reports created in TRENDSTAR and Horizon Performance Manager. You should take advantage of the masking options in those systems to remove unnecessary identifiers from data before sending the reports to Horizon Business Insight.

Then, in Horizon Business Insight:

- the Highlight Editor can be used to manage the contents of Horizon Business Insight highlights created from TRENDSTAR or Horizon Performance Manager reports.
- the Administrator's **Group Access** or **User Access** options can be used to control the access to Horizon Business Insight highlights, reports and resources that contain Protected Health Information.

Horizon Business Insight Information

- *Horizon Business Insight User's Guide*
  - refer to the chapter entitled, "Using the Administrator" for information on granting access to Horizon Business Insight objects.
- Administrator online help
  -

Uses and Disclosures: Consent and Authorizations

Standards

Sections **164.506**, **164.508**, **164.510**, **164.512** and **164.520** outline the requirements for consent and authorization to use or disclose protected health information.

Activities Related to Horizon Business Insight

If you capture information to track consents, authorizations, distribution of Notice of Privacy Practices, etc., you can consider distributing this information using Horizon Business Insight.

Use and Disclosures for Facility Directories/Clergy Lists

Standard

Section **164.510(a)** states that use and disclosure for facility directories is permitted except when an objection is expressed in accordance with previously stated rules.

Activities Related to Horizon Business Insight

Performance Analytics is not intended to support facility directories. If you choose to use it for this purpose, you will need to ensure that any patients who have “opted-out” are excluded from the directory.

Other Requirements Relating to Uses and Disclosures of Protected Health Information

Standard

Section **164.514(b)(2)(i)** lists the identifiers of the individual or of relatives, employers, or household members of the individual that should be removed in order to determine that health information is not individually identifiable.

Activities Related to Horizon Business Insight

Horizon Business Insight can be used to control the distribution of reports created in TRENDSTAR and Horizon Performance Manager. You should take advantage of the masking options in those systems to remove unnecessary identifiers from data before sending the reports to Horizon Business Insight.

Then, in Horizon Business Insight:

- the Highlight Editor can be used to manage the contents of Horizon Business Insight highlights created from TRENDSTAR or Horizon Performance Manager reports.
- the Administrator's **Group Access** or **User Access** options can be used to control the access to Horizon Business Insight highlights, reports and resources that contain Protected Health Information.

Horizon Business Insight Information

- *Horizon Business Insight User's Guide*
  - refer to the chapter entitled, "Using the Administrator" for information on granting access to Horizon Business Insight objects.
- Administrator online help

Confidential Communications Requirements

Standard

Section **164.522(b)(1)** requires entities to permit individuals to request to receive communications of protected health information from the covered health care provider by alternative means or at alternative locations. Covered entities must accommodate such reasonable requests.

Activities Related to Horizon Business Insight

If you are using Horizon Business Insight to distribute this information, it is the responsibility of the covered entity to make sure that the source system collects this information and that TRENDSTAR or Horizon Performance Manager are configured correctly to report and send it to Horizon Business Insight.