TIBCO LogLogic® Compliance Suite - HIPAA Edition
Guide

Software Release 3.9.0
November 2017
Document Updated: April 2018

Two-Second Advantage®

TIBCO®

Important Information

This document contains excerpted portions of the Health Insurance Portability and Accountability Act ("HIPAA") regulations (collectively, the "Regulatory Language"). The Regulatory Language is provided by TIBCO solely for your convenience and to provide context for certain functionality of the TIBCO LogLogic® products. The inclusion or omission by TIBCO of any Regulatory Language is in no way intended as legal advice regarding the HIPAA regulations and does not constitute any representation or warranty that any TIBCO products comply with the terms contained in such Regulatory Language. If you have additional questions about the HIPAA regulations, you should consult with an attorney for further legal guidance.

Contents

Figures

TIBCO Documentation and Support Services

How to Access TIBCO Documentation

Documentation for TIBCO products is available on the TIBCO Product Documentation website, mainly in HTML and PDF formats.

The TIBCO Product Documentation website is updated frequently and is more current than any other documentation included with the product. To access the latest documentation, visit https://docs.tibco.com.

Product-Specific Documentation

The following documents for this product can be found on the TIBCO Documentation site:

- *TIBCO LogLogic® Compliance Suite - HIPAA Guide*
- *TIBCO LogLogic® Compliance Suite - HIPAA Readme*
- *TIBCO LogLogic® Compliance Suite - HIPAA Release Notes*

How to Contact TIBCO Support

You can contact TIBCO Support in the following ways:

- For an overview of TIBCO Support, visit http://www.tibco.com/services/support.
- For accessing the Support Knowledge Base and getting personalized content about products you are interested in, visit the TIBCO Support portal at https://support.tibco.com.
- For creating a Support case, you must have a valid maintenance or support contract with TIBCO. You also need a user name and password to log in to https://support.tibco.com. If you do not have a user name, you can request one by clicking Register on the website.

How to Join TIBCO Community

TIBCO Community is the official channel for TIBCO customers, partners, and employee subject matter experts to share and access their collective experience. TIBCO Community offers access to Q&A forums, product wikis, and best practices. It also offers access to extensions, adapters, solution accelerators, and tools that extend and enable customers to gain full value from TIBCO products. In addition, users can submit and vote on feature requests from within the TIBCO Ideas Portal. For a free registration, go to https://community.tibco.com.

Establishment of IT Controls for the HIPAA Security Rule

The Health Insurance Portability and Accountability Act (HIPAA) law, passed in 1996, is designed to allow employees to change jobs without concern about continuation of health insurance coverage, provide improved access to health insurance for patients, reduce inefficiencies in the health care industry and protect the electronic health information of patients.

This document identifies how the TIBCO LogLogic Compliance Suite satisfies specific requirements of the HIPAA security rule which directs that:

- The Department of Health and Human Services (HHS) Medicare Program,
- Other Federal agencies operating health plans or providing health care,
- State Medicaid agencies,
- Private health plans,
- Health care providers and
- Health care clearinghouses

assure their patients that the integrity, confidentiality, and availability of Electronic Protected Health Information they collect, maintain, use, or transmit is protected. Today, the amount of electronic health information is staggering and its integrity, confidentiality and availability are threatened by worms, viruses, unauthorized disclosure and misuse.

The HIPAA Security Rule requires that Covered Entities implement various standards to safeguard electronic health information. HIPAA implementation standards are either required (R) or addressable (A). If an Implementation Specification is “required”, the Covered Entity must implement the Implementation Specifications. If the Implementation Specification is “addressable” the Covered Entity must:

Assess whether each Implementation Specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the entity’s Electronic Protected Health Information; and as applicable to the entity

- Implement the Implementation Specification if reasonable and appropriate; or
- If implementing the Implementation Specification is not reasonable and appropriate
  - Document why it would not be reasonable and appropriate to implement the Implementation Specification
  - Implement an equivalent alternative measure if reasonable and appropriate

A large portion of the HIPAA Security Rule Standards and Implementation Specifications can be directly satisfied or enhanced by use of the TIBCO LogLogic Compliance Suite. This document explains which HIPAA Standards and Implementation Specifications are satisfied by the TIBCO LogLogic Compliance Suite and how.

Satisfied HIPAA Implementation Specifications

HIPAA’s Security Rule contains over 40 implementation specifications covering areas including Administrative Safeguards and Technical Safeguards.

Twenty HIPAA implementation specifications were identified that can be evidenced or audited by TIBCO LogLogic reports and alerts.

Standards	Sections	Implementation Specification (R) = Required, (A) = Addressable, (N/A) = Not Available
164.308 - Administrative Safeguards		
Workforce Security	164.308(a)(3)	Authorization and Supervision (A) Termination Procedures (A)
Information Access Management	164.308(a)(4)	Isolating Health Care Clearinghouse Function (R) Access Authorization (A) Access Establishment and Modification (A)
Security Awareness and Training	164.308(a)(5)	Security Reminders (A) Log-in Monitoring (A) Password Management (A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)
Contingency Plan	164.308(a)(7)	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedures (A)
164.312- Technical Safeguards		
Access Control	164.312(a)(1)	Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A)
Audit Controls	164.312(b)	N/A
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication	164.312(d)	N/A

Other Implementation Specifications

Although some of the implementation specifications are not directly related to log data, the TIBCO LogLogic reports and alerts can be used to assist in satisfying those requirements. For example, even though log data are not directly used in HIPAA section 164.308(a)(1), Security Management Process, routinely reviewing TIBCO LogLogic reports and responding to TIBCO LogLogic alerts aids in preventing, detecting, containing and correcting security violations.

The data generated by the TIBCO LogLogic Compliance Suite can be used to conduct a thorough risk analysis of the risks and vulnerabilities threatening the entity. The risk analysis can then be used to

customize specific TIBCO LogLogic reports and alerts that enable an entity to manage risks in a dynamic environment where risks and vulnerabilities rapidly change.

All TIBCO LogLogic reports can be used to monitor regular user activity, as well as the activity and results of system and network administrators. Any activity or network configuration setting that is determined to violate security policies or procedures can result in sanctions against people, processes or resources. All TIBCO LogLogic reports and alerts directly aid an entity by allowing the regular review of information system activity.

The LogLogic® Compliance Suite - HIPAA Edition allows for the continuous monitoring of the IT infrastructure using behavioral-based alerts. Configure alerts to monitor performance of firewalls, routers, switches, servers, applications, and operating systems so they can be notified immediately of failures. real-time reports and custom, regular-expression searches also enable administrators to quickly identify and determine the root cause of any problems. This further mitigates risk and minimizes interruptions to service availability.

HITECH Sec. 1340199(a) Application of Security Provisions

Security provisions, penalties, and additional guidance on the provisions are discussed in HITECH Sec. 1340199(a) Application of Security Provisions and Penalties to Business Associates of Covered Entities; Annual Guidance on Security Provisions. Application of Security Provisions—Sections 164.308, 164.310, 164.312, and 164.316 of title 45, Code of Federal Regulations, shall apply to a business associate of a covered entity in the same manner that such sections apply to the covered entity. The additional requirements of this title that relate to security and that are made applicable with respect to covered entities shall also be applicable to such a business associate and shall be incorporated into the business associate agreement between the business associate and the covered entity.

The LogLogic® Compliance Suite - HIPAA Edition Overview

The LogLogic® Compliance Suite - HIPAA Edition delivers automated process validation, reporting and alerts based on infrastructure data to evidence and enforce business, and IT policies related to compliance. By automating compliance reporting and alerting based on critical infrastructure data collected and stored by TIBCO LogLogic's Appliances, the TIBCO LogLogic Compliance Suite removes the complexity and resource requirements for implementing HIPAA security standards and implementation specifications.

TIBCO LogLogic's Compliance Suite:

- Automates compliance activities and dramatically improves audit accuracy.
- Provides risk assessment data and reduces the time to mitigate the risk factor.
- Allows organizations to use infrastructure data to provide evidence of and enforce IT controls.
- Provides industry-leading reporting depth and breadth, including real-time reporting and alerting on HIPAA compliance.
- Delivers over 353 out-of-the-box Compliance Reports and more than 130 out-of-box Alerts with executive-level views.
- Enables customization of any Compliance Report to map reports against your company's policies.

Organizations can use the LogLogic® Compliance Suite - HIPAA Edition to:

- Enforce controls using TIBCO LogLogic technologies.
- Show auditors alerts and reports to prove your compliance status with TIBCO LogLogic.
- Monitor continuously with TIBCO LogLogic to ensure continuous compliance.
- Provide auditors TIBCO LogLogic unaltered evidence of log data review and follow-up.
- Provide assurances of the integrity of the log data collected and reports.

Compliance Categories

Log data allows organizations to manage the extreme challenges of meeting major HIPAA implementation specifications. TIBCO LogLogic's compliance reports and alerts satisfy the following categories:

- Identity and Access
- Monitoring and Reporting
- Change Management
- Security Management
- Availability Management
- Continuity Management

Identity and Access

The LogLogic® Compliance Suite - HIPAA Edition includes reports and alerts to show that all HIPAA-related systems (that is, networks, applications, and databases) are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data.

The risks of non-compliance might result in an unauthorized or inappropriate access to key systems, which may negatively impact the security, integrity, accuracy and completeness of healthcare information.

Monitoring and Reporting

The LogLogic® Compliance Suite - HIPAA Edition includes reports and alerts to allow customers to continuously monitor the IT infrastructure for any security violations. Reports are provided in a format meaningful to the stakeholders. The monitoring statistics should be analyzed and acted upon to identify negative and positive trends for individual services as well as for services overall.

The risks of non-compliance in this area could significantly impact service availability and security of the IT infrastructure, which may negatively impact the security, integrity, accuracy, and completeness of healthcare information.

Change Management

The LogLogic® Compliance Suite - HIPAA Edition includes reports and alerts to show that all systems and system changes are appropriately requested, approved, tested, and validated by authorized personnel prior to implementation to the production environment. These reports and alerts can also show that division of roles and responsibilities have been implemented to reduce the possibility for a single individual to subvert a critical process. Management must make sure that the personnel are performing only authorized duties relevant to their respective jobs and positions.

The risks of non-compliance might result in unauthorized changes or an improper roll-out of new source code to key systems. This might negatively impact the security, integrity, accuracy, and completeness of healthcare information.

Security Management

The LogLogic® Compliance Suite - HIPAA Edition includes reports and alerts to show that all network security devices, including firewalls which control computer traffic into a company's network, as well as IDS systems which monitor the computer traffic, have been configured appropriately to allow only the requested and approved traffic in and out of the network.

The risks of non-compliance may result in unauthorized access from the Internet. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

Availability Management

The LogLogic® Compliance Suite - HIPAA Edition includes reports and alerts to monitor the availability of critical IT infrastructure components. Alerts can be setup to monitor when critical components are sending abnormal amount of log data, which could indicate attacks on the component or that there's system errors, or have stopped sending log data, which could indicate failure of these components.

The risk of non-compliance could significantly impact the business viability and could prevent an organization from recording healthcare transactions and thereby undermine its integrity.

Continuity Management

The LogLogic® Compliance Suite - HIPAA Edition includes reports and alerts to monitor that data are backed up on a regular basis. Reports can be automatically generated to ensure that backups and restores are performed successfully. Deficiencies in this area could impact the resilience of the infrastructure and the availability of critical resources.

TIBCO LogLogic Compliance Suite Setup

Setting up the LogLogic® Compliance Suite - HIPAA Edition comprises checking that all prerequisites are met before starting the installation process, installing the Compliance Suite file, and enabling the alerts.

See Installing the Compliance Suite and Enabling Compliance Suite Alerts for more details.

Installing the Compliance Suite

Prerequisites

Before installing the LogLogic® Compliance Suite - HIPAA Edition, ensure that you have:

- TIBCO LogLogic LX or MX or ST Appliance running TIBCO LogLogic Release 5.7.x or higher
- TIBCO LogLogic® Log Source Packages (LSP) 32.1 or 33 installed

The Compliance Suite includes one file containing HIPAA filters, custom reports, and alerts.

- `hipaa.xml`
  – HIPAA Reports, Search Filters, and Alerts

If you have previously imported any earlier versions of the Compliance Suite files, importing this version of the Compliance Suite will not overwrite the original files or any changes that have been made, unless you have saved the changes to the object using the default name.

If you have made any changes to base Compliance Suite alerts, search filters, or custom reports, TIBCO recommends saving these items with non-default names. This will help ensure that the latest Compliance Suite updates can be installed without any compatibility issues or naming conflicts.

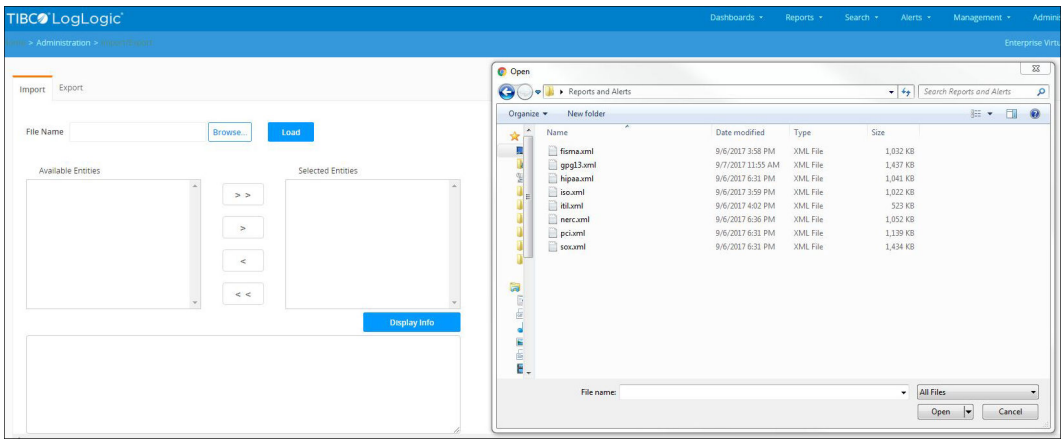
Procedure

1. Log in to your TIBCO LogLogic LX or MX or ST Appliance as admin.
2. From the navigation menu, select **Administration** > **Import or Export** .

   The **Import** and **Export** tabs open.
3. Load the Compliance Suite file by completing the following steps:
   a) In the **Import** tab, click **Browse**.
   b) In the **File Upload** window, select the appropriate XML file and then click **Open**.

      The following figure shows the **File Upload** window that appears after clicking **Browse** on the **Import** tab.

Loading a Compliance Suite File



c) Click **Load**.

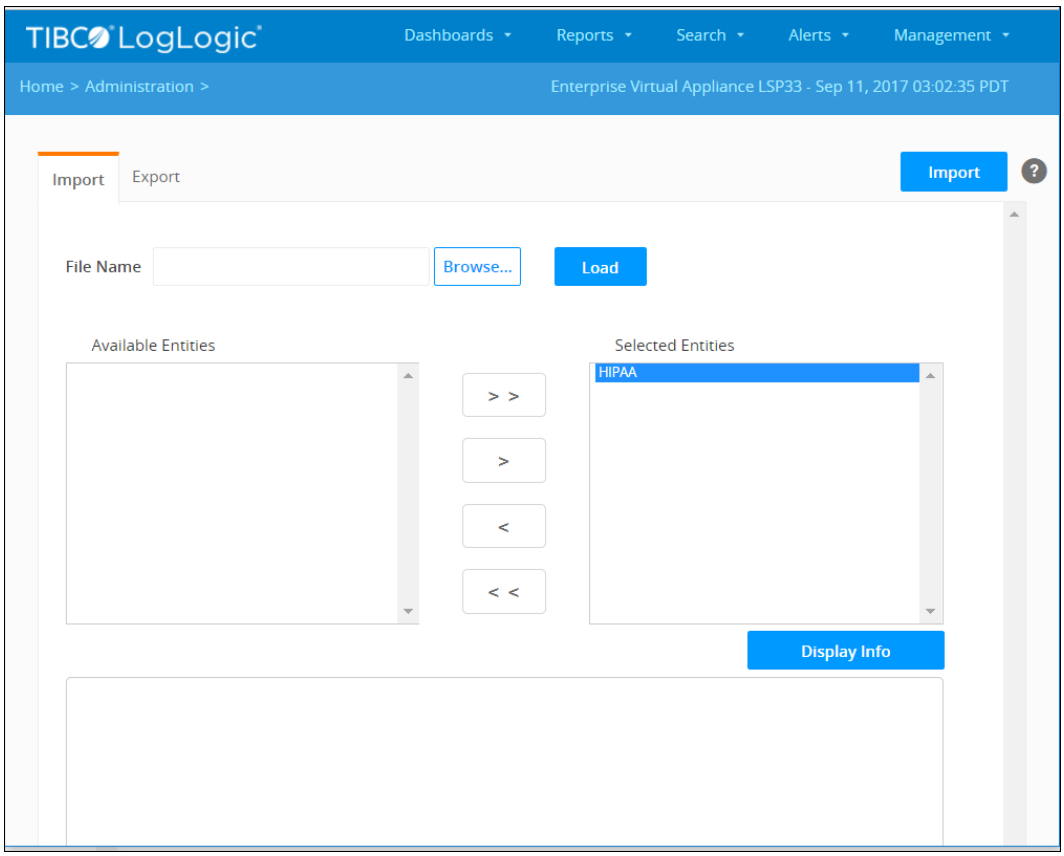
This loads the **Available Entities** from the XML file.

d) Click **Add All Entities**.

You can also select the specific HIPAA entity from the **Available Entities** text block and then click **Add Selected Entities**.

The following figure shows all entities of the HIPAA XML file that were selected by clicking **Add All Entities**.

Selected Entities to be Imported



4. Click **Import**.

An import successfully completed message appears above the **File Name** text field.

Installation is complete after the XML file is imported successfully.

The Compliance Suite Usage

Once you have successfully installed the LogLogic® Compliance Suite - HIPAA Edition, you can begin using the custom reports and alerts.

The following sections help you view, test, and modify, the packaged custom reports and alerts. The custom reports and alerts were designed to run out-of-the box; however, TIBCO LogLogic enables you to perform further customization if necessary.

The Compliance Suite Reports

All LogLogic® Compliance Suite - HIPAA Edition reports are designed to run out-of-the box as well as to be flexible if you have to make modifications based on your business needs.

For a description of all custom reports in this Compliance Suite, see TIBCO LogLogic Reports for HIPAA.

- Viewing Compliance Suite Reports and Output Data
- Customizing Compliance Suite Reports

Viewing Compliance Suite Reports and Output Data

Using TIBCO LogLogic LX or MX or ST Appliance, you can view all the Compliance Suite reports for the device and run them as well as view the output data.

Procedure

1. Log in to your TIBCO LogLogic LX or MX or ST Appliance as admin.
2. From the navigation menu, select **Reports** > **HIPAA** .

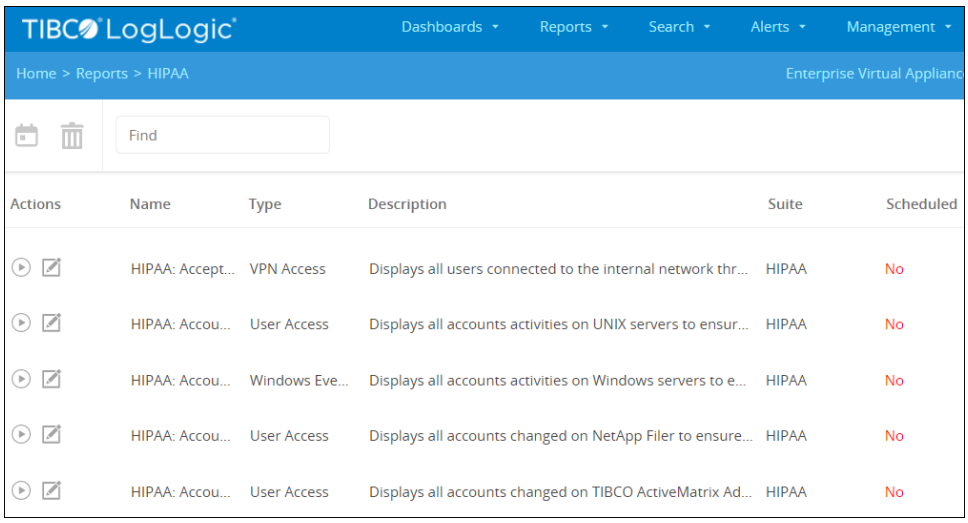
   

   You can also access all of your custom reports on the Appliance including the Compliance Suite reports you installed, by selecting **Reports** > **All Saved Reports** .
3. On the **Reports** page, you can see all of the custom reports you loaded during the installation process.

   You can navigate through all of the custom reports using the page navigation buttons at the top and bottom of the **Reports** page.

   The following figure shows a cropped list of the Compliance Suite reports loaded from the HIPAA XML file.

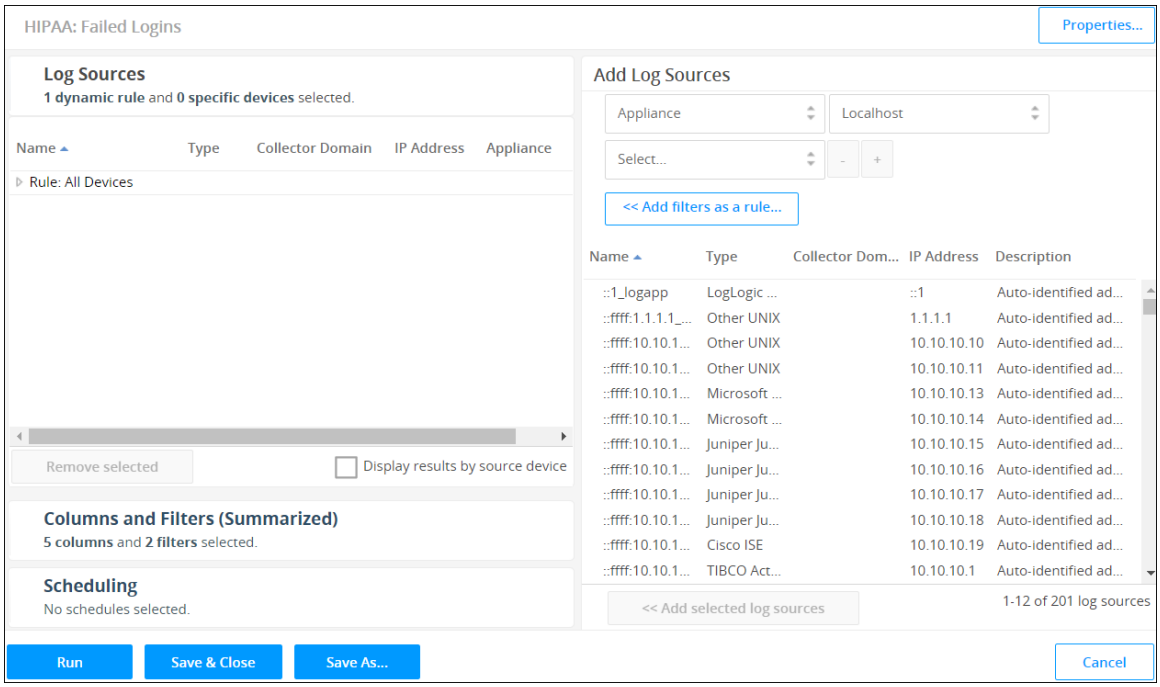
Compliance Suite Reports



4. Click the **Edit** button of a report to see details such as, the Appliance where the report runs, the associated device type, and when the report runs.
   a) To view the filter parameters, click **Columns and Filters**.
   b) To view details about a report such as the report name and description, click **Properties**.

   The following figure shows the details of the **HIPAA: Failed Logins** report.

   Failed Logins Report Details



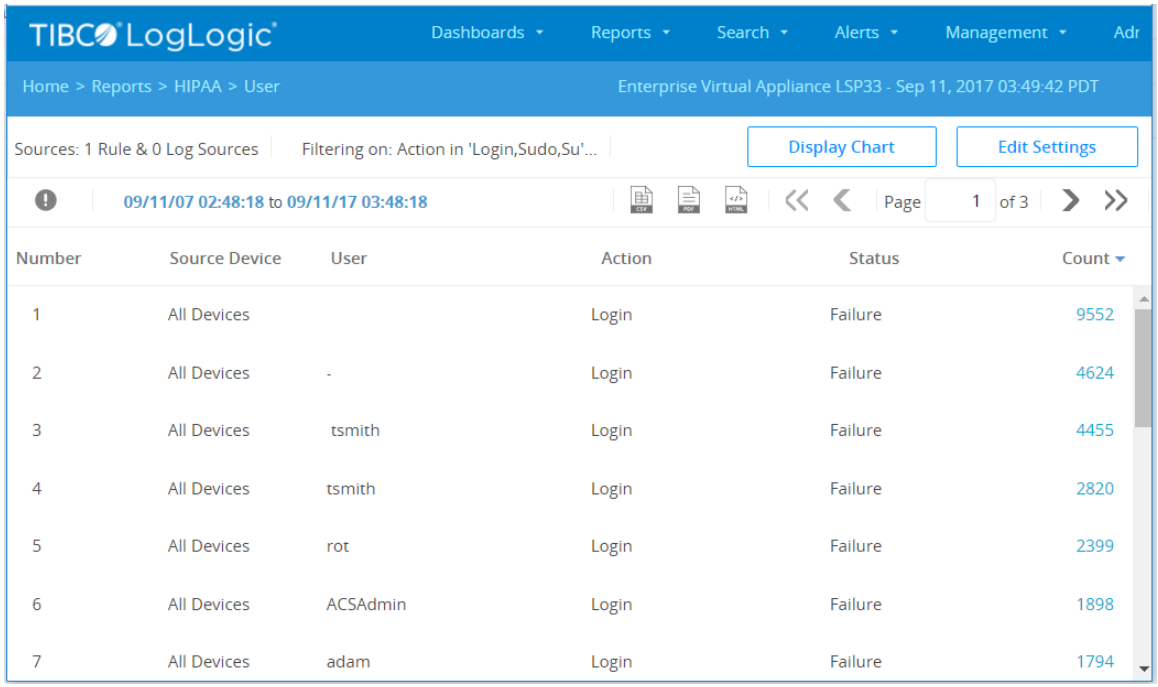
5. Run the report to view the report output data by completing the following steps:
   a) Click **Run**.

   The report runs and returns data based on the set parameters.
   b) To view detailed drill-down information, click the **Count** column link.

You can use the **Back to summarized results** button to return to the main data output view.

The following figure shows sample results from the **HIPAA: Failed Logins** report.

Failed Logins Report Results



If you want to modify the main data output view, you can modify the report parameters and then run the report again.

Customizing Compliance Suite Reports

The LogLogic® Compliance Suite - HIPAA Edition reports are designed to run out-of-the-box to meet specific compliance requirements. However, you may want to modify the reports to include additional information or devices depending on your business needs.

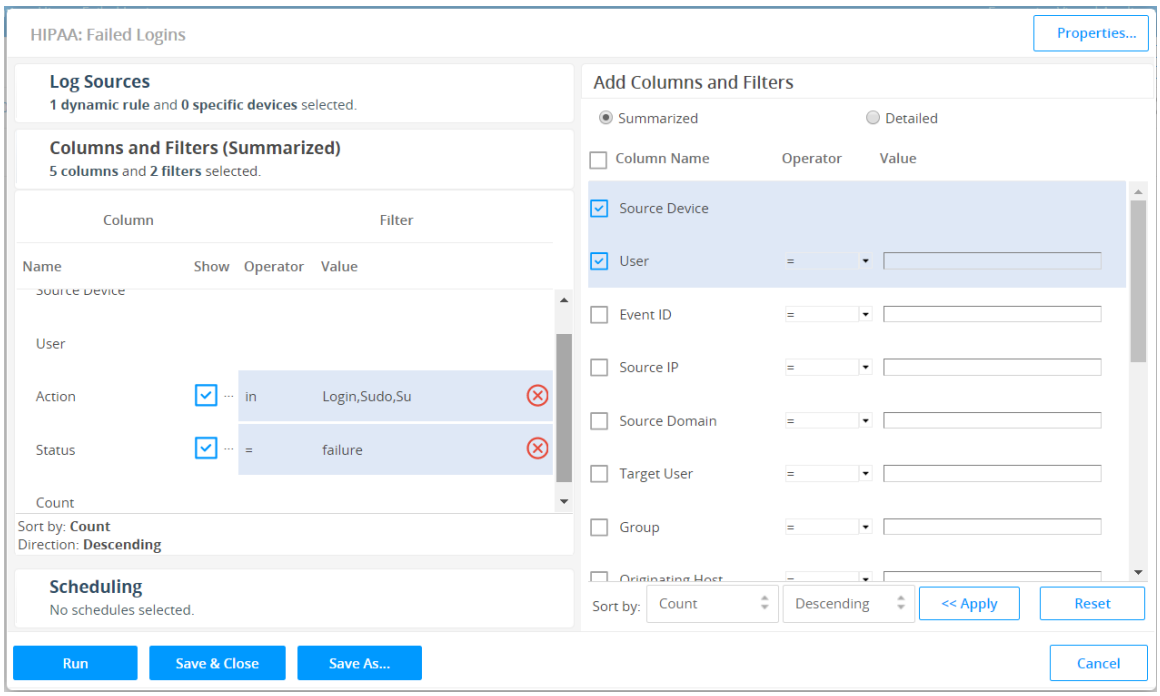
Procedure

1. Make sure that you are on the **Reports** page and click the **Edit** button for a report you want to modify.
2. Modify the report details (that is, name, description, and so on), filters, and parameters.

   TIBCO LogLogic enables you to customize everything pertaining to the summarization and presentation of the reports. You can modify the device on which the report runs, schedule when the report runs, and set specific report search filters.

   The following figure shows the report filters available under **Columns and Filters** options.

Advanced Options and Update Saved Custom Report Views



It is a good practice to test your modifications to ensure that the report meets your business needs.

3. To test the report, click **Run**.

   The report runs and returns data based on the set parameters. Verify that the returned data is what you want. Continue modifying and testing the report as needed.

4. Save the report:
   a) Click **Save As**.

      Make any necessary modifications to the report details (that is, **Report Name**, **Report Description**, and so on).
   b) Click **Save & Close**.

      A report saved message appears. Your report is now modified. Consider testing the output of the report again to ensure you are returning all of the data you need from this report.

The Compliance Suite Alerts

The LogLogic® Compliance Suite - HIPAA Edition alerts enable you to manage activities helping you to maintain HIPAA compliance. Activities can include detecting unusual traffic on your network or detecting Appliance system anomalies.

By default, the Compliance Suite alerts are disabled so that you can configure your environment with only those alerts that are necessary. For a description of all alerts in this Compliance Suite, see TIBCO LogLogicAlerts for HIPAA.

- Accessing Available Compliance Suite Alerts
- Enabling Compliance Suite Alerts
- Viewing Compliance Suite Alert Results

Accessing Available Compliance Suite Alerts

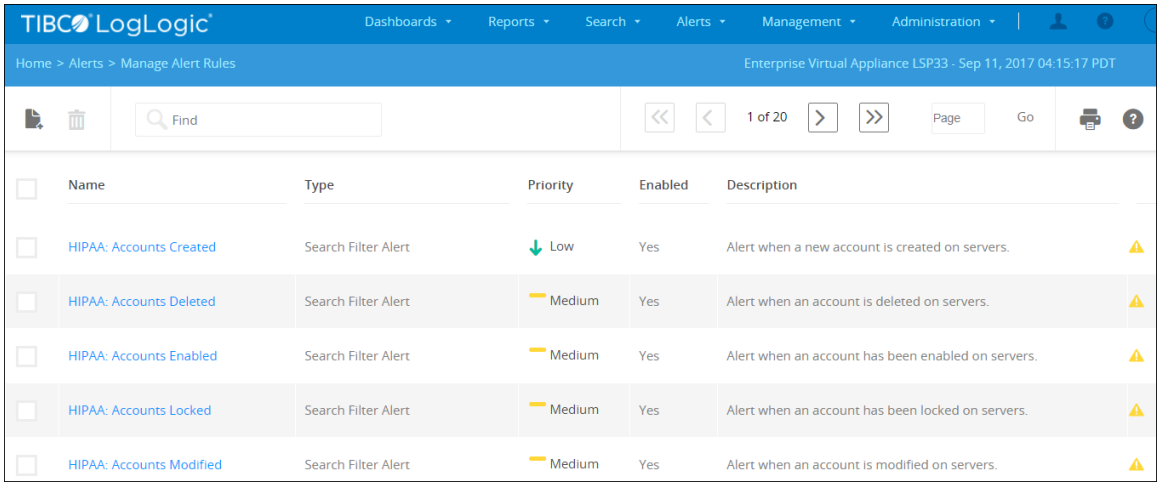
The Compliance Suite package contains a number of alerts that you can easily enable and modify for your business needs.

Procedure

1. From the navigation menu, click **Alerts** > **Manage Alert Rules** .

   The following figure shows a cropped list of the Compliance Suite alerts loaded from the HIPAA XML file.

   Compliance Suite Alerts



2. To view details of a specific alert, click the **Name** of the alert.

   The **General** tab is selected by default, but each tab on the page contains information required to enable an alert.

3. Click on each of the tabs to view the default entries.

   Make sure that you identify the default entries and areas that might need to be modified.

Enabling Compliance Suite Alerts

By default, the compliance suite alerts have pre-configured information to help you get started. In some instances, you can simply enable the alert because the default settings are aimed at capturing a broad range of alerts.

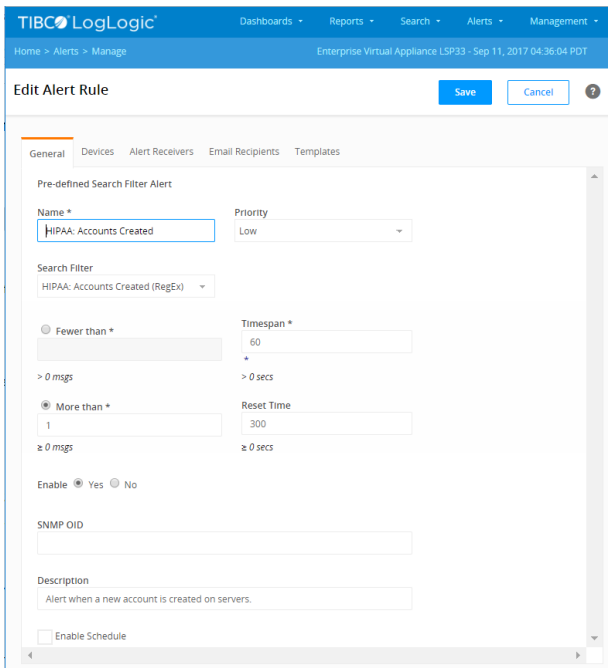
To enable alerts, you must set the device to monitor, the SNMP trap receivers, as well as who receives an alert notification and how they receive it.

Procedure

1. From the navigation menu, select **Alerts** > **Manage Alert Rules** .
2. Click the **Name** of the alert.
3. On the **General** tab, for **Enable** select the **Yes** radio button.

   The following figure shows the **General** tab for the **HIPAA: Accounts Created** alert.

Accounts Created Alert

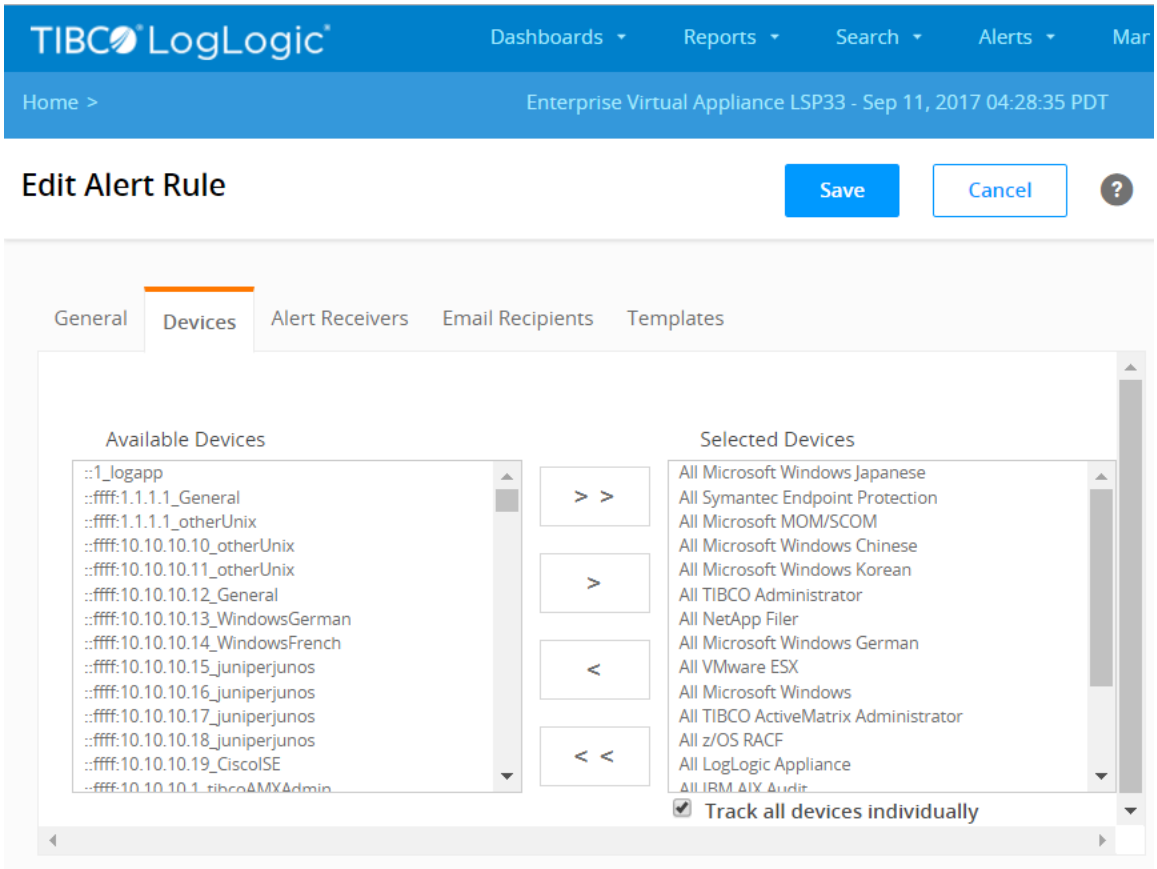


4. Select the device to be alerted on by completing the following steps. You can define alerts for all devices, a selection of devices, or a single device.
   a) Select the **Devices** tab.
   b) In the **Available Devices** text block, select the appropriate log sources (that is, devices) you want to monitor and be alerted on when an alert rule is triggered.

      If the **Show Only Device Groups** setting is enabled on the Appliance, then the **Available Devices** text block lists only device groups. To enable or disable this feature, go to **Administration** > **System Settings** > **General** tab, scroll down to the **System Performance Settings** section and modify the **Optimize Device Selection List** option
   c) Click **Add All** or **Add Selected Device(s)**.

      The following figure shows the **Devices** tab for the selected alert.

Available and Selected Devices



5. The Appliance has the ability to generate an SNMP trap that is sent to an SNMP trap receiver when an alert rule is triggered. Select the alert receivers available to your device by completing the following steps:
   a) Select the **Alert Receivers** tab.
   b) In the **Available Alert Receivers** text block, select the appropriate alert receivers available for your device(s).
   c) Click **Add All** or **Add Selected Receiver(s)**.
6. Select the email recipients to be alerted with a notification email when an alert rule is triggered by completing the following steps:
   a) Select the **Email Recipients** tab.
   b) In the **Available Users** text block, select the appropriate email recipients.

      The **Available Users** text block lists all of the user accounts on the Appliance.
   c) Click **Add All** or **Add Selected User(s)**.
7. Click **Update**.

Viewing Compliance Suite Alert Results

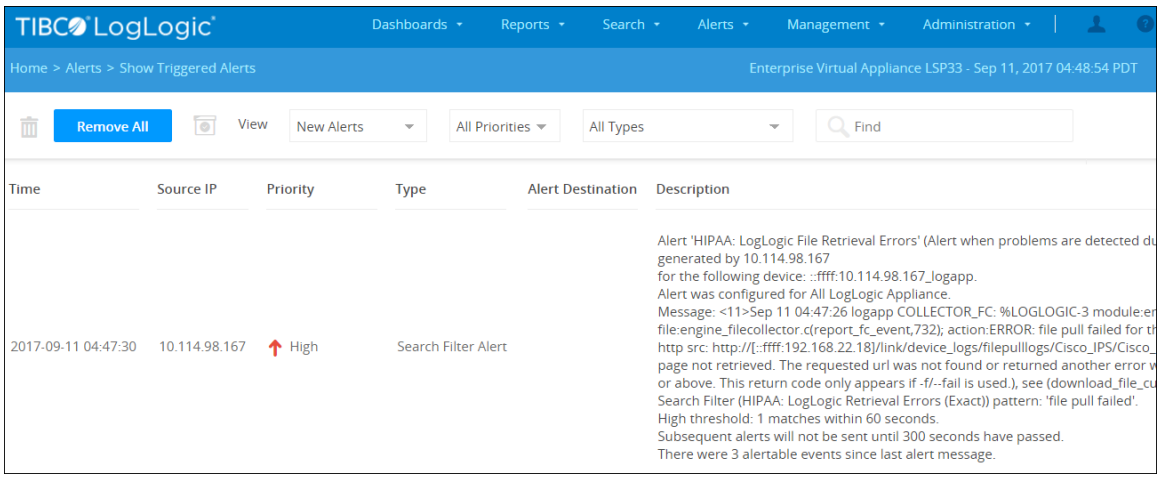
After you have enabled at least one alert, and that alert is triggered, you can view the results.

Procedure

1. In the navigation menu, select **Alerts** > **Show Triggered Alerts** .

   The following figure shows a cropped version of the **Show Triggered Alert** page.

Aggregated Alert Log



2. From the **Show** drop-down menu, select the desired alert and priority filters to show only those alerts you want to display. The defaults are **New Alerts** and **All Priorities**.
3. (Management Station Appliances Only) From the **From Appliance** drop-down menu, select the Appliance from which you want to view the alerts.
4. View the results of your query. You can navigate through all of the data by using the page navigation buttons or the page text field.
5. You can either acknowledge or remove an alert. Click the check box next to the alert name, then click either **Acknowledge**, **Remove**, or **Remove All**.

Each alert was triggered based on your set alert parameters, so care must be taken when acknowledging or removing the alert.

HIPAA Security Rule Implementation Specifications

This section provides planning and implementation information for HIPAA security rule implementation specifications. It also provides a brief listing of TIBCO LogLogic Compliance Suite reports and alerts that are applicable to those specifications.

164.308(a)(3) Workforce Security

Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

Implementation Specification	Description
164.308(a)(3)(ii)(A)	**Authorization and Supervision (Addressable)** Implement procedures for the authorization and supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
164.308(a)(3)(ii)(C)	**Termination Procedures (Addressable)** Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.

164.308(a)(3)(ii)(A) – Authorization and Supervision

Implement procedures for the authorization and supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

Illustrative Controls and TIBCO LogLogic Solution

User access rights to systems and data should be in line with defined and documented business needs and job requirements.

Accurately managing user access rights addresses the issues of unintended or malicious modifications of healthcare data. Deficiencies in this area might allow unauthorized modifications that could lead to errors in reporting.

Administrators must determine that the following requirements are met:

- Access rights for privileged User IDs are restricted to least privileges necessary to perform the job.
- Assignment of privileges to individuals is based on job classification and function.
- Requirement for an authorization form that is signed by management and specifies required privileges.
- An automated access control system is being used.
- “Deny-all” setting by default.

To satisfy this control objective, administrators must monitor and verify that all user access to programs and data, and periodically review the user access to files and programs to ensure the users have not accessed items outside of their role. Administrators must select a sample of users who have logged in to healthcare reporting servers and review their access for appropriateness based upon their job functions.

As part of the procedures for the authorization and supervision of workforce members who work with electronic protected health information, TIBCO LogLogic access reports and alerts must be used to validate that the access has been configured correctly and appropriate access is maintained.

Reports and Alerts

Use the following link or reference to see the 164.308(a)(3)(ii)(A) reports and alerts: 164.308(a)(3)(ii)(A) – Authorization and Supervision.

164.308(a)(3)(ii)(C) – Termination Procedures (Addressable)

Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in the Workforce clearance procedures paragraph of section 164.308.

Illustrative Controls and TIBCO LogLogic Solution

Administrators must demonstrate that user access privileges are modified and revoked in a timely manner upon job change or termination. Review reports and alerts on account activities, accounts created or deleted, group members added or deleted, and successful logins to VPN concentrators and critical servers.

Take expedient actions regarding job changes, especially job terminations. Knowledge transfer needs to be arranged, responsibilities reassigned and access rights removed such that risks are minimized and continuity of the function is guaranteed. When a person changes jobs or is terminated from a company, user access privileges must be modified according to the company's business guidelines.

To satisfy this requirement, administrators must periodically ensure that only current and authorized employees have access to electronic protected health information systems. Administrators must ensure that all terminated users have been disabled. In addition, administrators must ensure that logins to servers as well as permissions assigned to users who changed jobs are appropriate for the new role they are in.

To ensure that the requirements listed in the preceding section are met, administrators must review reports of all user deletions and group member modifications. This ensures that terminated users are removed and users who changed jobs have been removed from the appropriate groups.

TIBCO LogLogic access reports and alerts that detail accounts and groups being removed are used to validate that access to electronic protected health information has been terminated as part of this addressable Implementation specification. Access reports and alerts are reviewed to ensure that anyone terminated does not retain access or has any system or network activity following the termination.

Reports and Alerts

Use the following link or reference to see the 164.308(a)(3)(ii)(C) reports and alerts: 164.308(a)(3)(ii)(C) – Termination Procedures (Addressable).

164.308(a)(4) Information Access Management

Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the application requirements of subpart E of this part.

Implementation Specification	Description
164.308(a)(4)(ii)(A)	**Isolating Health Care Clearinghouse Functions (Required)** If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.
164.308(a)(4)(ii)(B)	**Access Authorization (Addressable)** Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.
164.308(a)(4)(ii)(C)	**Access Establishment and Modification (Addressable)** Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

164.308(a)(4)(ii)(A) - Isolating Health Care Clearinghouse Functions (Required)

If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.

Illustrative Controls and TIBCO LogLogic Solution

Administrators must identify all servers and applications related to health care clearinghouse have been properly isolated from the rest of the organization. The most prevalent method of isolating these functions is to use firewalls to protect the related servers and applications.

Administrators must identify all changes to firewall and router configurations and ensure that a formal process is in place for all changes, including management approval and testing for all changes to external network connections and the firewall configurations. Administrators must also ensure all changes are authorized and that rule sets are periodically reviewed.

The most efficient way to identify configuration changes is at the time of the modification. Administrators must set up alerts so that any changes to the configuration of network systems and devices, authorized or otherwise, are detected and notified.

Administrators must periodically review all firewall rules to ensure an accurate access control list. Administrators must correlate network traffic with the firewall policy to validate that the appropriate rules are in place to protect the company.

In addition, no firewall in any company must allow the use of any known risky services or protocol. These known risky services provide intruders an easy way into the company.

Administrators must identify all protocols and services that are considered risky to pass through the firewall. These risky services include, but not limit to, FTP (21/tcp), Telnet (23/tcp), Rlogin (513/tcp), Rsh (514/tcp), Netbios (137-139/tcp,udp), and others. Any risky protocols or services must be immediately removed from the firewall policies.

TIBCO LogLogic reports and alerts augment processes and procedures to protect electronic health information from a larger organization by recording and reporting on the addition of new users from the larger organization on clearinghouse servers and systems and attempted access from other network segments.

Reports and Alerts

Use the following link or reference to see the 164.308(a)(4)(ii)(A) reports and alerts: 164.308(a)(4)(ii)(A) - Isolating Health Care Clearinghouse Functions (Required).

164.308(a)(4)(ii)(B) - Access Authorization (Addressable)

Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

Reports and Alerts

Use the following link or reference to see the 164.308(a)(4)(ii)(B) reports and alerts: 164.308(a)(4)(ii)(B) - Access Authorization (Addressable).

164.308(a)(4)(ii)(C) - Access Establishment and Modification (Addressable)

Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

Illustrative Controls and TIBCO LogLogic Solution

Set up real-time alerts to detect any unauthorized or unapproved changes to users or groups. Monitor account management activities such as user or group addition, deletion, or modification to ensure all user access privileges are appropriate and approved.

Requesting, establishing, issuing, suspending, modifying, and closing user accounts and related user privileges are addressed by user account management. An approval procedure requiring the data or system owner to grant access privileges to new and existing users should be included. These procedures apply to all users, including administrators (privileged users), internal and external users, in both normal and emergency situations. Rights and obligations relative to access to enterprise systems and information are contractually arranged for all types of users.

Perform regular management review of all accounts and related privileges. Demonstrate that procedures exist for the registration, change, and deletion of users from electronic protected health information systems and subsystems on a timely basis and confirm that the procedures are followed. Procedures must exist and be followed to ensure timely action relating to requesting, establishing, issuing, suspending, and closing user accounts.

To satisfy this requirement, administrators must ensure that permissions have been granted to the appropriate users, and to ensure that all network and application access requests are adequately documented and approved by appropriate Management personnel. As proof, administrators can select a sample of terminated employees and to ensure the accounts for these employees have been terminated in a timely manner. Administrators must review reports that detail the access policy on all servers and applications. They must be configured to ensure password policies are enforced and access activity recorded.

Server and application logs must be reviewed to ensure passwords are changed periodically and in accordance with corporate policy.

TIBCO LogLogic reports augment processes and procedures for granting access by allowing the validation of new users, elevated privileges on network devices and systems that provide access to electronic health information. The addition or modification of accounts captured by the TIBCOLogLogic Compliance Suite provides specific information about who has access to electronic health information. You can also monitor account activities to ensure that access is implemented

appropriately. Special access through VPNs, the Internet, and other subnets can also validate that remote access privileges are implemented as desired.

Reports and Alerts

Use the following link or reference to see the 164.308(a)(4)(ii)(C) reports and alerts: 164.308(a)(4)(ii)(C) - Access Establishment and Modification (Addressable).

164.308(a)(5) Security Awareness and Training

Implement a security awareness and training program for all members of its workforce (including management).

Implementation Specification	Description
164.308(a)(5)(ii)(A)	**Security Reminders (Addressable)** Periodic security updates.
164.308(a)(5)(ii)(C)	**Log-In Monitoring (Addressable)** Procedures for monitoring log-in attempts and reporting discrepancies.
164.308(a)(5)(ii)(D)	**Password Management (Addressable)** Procedures for creating, changing, and safeguarding passwords.

164.308(a)(5)(ii)(A) – Security Reminder (Addressable)

Periodic security updates.

Illustrative Controls and TIBCO LogLogic Solution

Security patch management is the process of deploying interim security updates or software releases into the production environment. The goal of security patches is to help the organization maintain the system and data integrity and ensure appropriate access. It helps organizations to maintain operational efficiency and effectiveness, overcome security vulnerabilities, and maintain the stability of your production environment.

A number of security vulnerabilities can exist in the IT environment that can be exploited and lead to loss of revenue and/or intellectual property. Organizations must determine and maintain a known level of trust within the IT environment and ensure that vendor-supplied security patches have been properly tested and installed within a reasonable period of time. Failure to do so could lead to impacts such as downtime, remediation time, questionable data integrity, loss of credibility, negative public relations, legal defenses, and stolen intellectual property.

To satisfy this requirement, administrators must periodically review to ensure all security patches have been installed on critical servers.

Reports and Alerts

Use the following link or reference to see the 164.308(a)(5)(ii)(A) reports and alerts: 164.308(a)(5)(ii)(A) – Security Reminder (Addressable).

164.308(a)(5)(ii)(C) - Log-in Monitoring (Addressable)

Procedures for monitoring log-in attempts and reporting discrepancies.

Illustrative Controls and TIBCO LogLogic Solution

To establish user identification, implement authentication, and enforce access rights, you must deploy cost-effective technical and procedural measures and keep them current. All logins to network devices, operating systems, databases, and applications must be reviewed to ensure only authorized and appropriate personnel have access. Monitor and verify all user access to programs and data. Review access to ensure segregation of duties as well that all privileges are properly assigned and approved.

To satisfy this control objective, administrators must assess the authentication mechanisms used to validate user credentials (new and existing) for healthcare reporting systems to support the validity of transactions. Server and application activities must be monitored for locked-out and enabled accounts as they can represent malicious activities.

Reports and Alerts

Use the following link or reference to see the 164.308(a)(5)(ii)(C) reports and alerts: 164.308(a)(5)(ii)(C) - Log-in Monitoring (Addressable).

164.308(a)(5)(ii)(D) - Password Management (Addressable)

Procedures for creating, changing, and safeguarding passwords.

Illustrative Controls and TIBCO LogLogic Solution

Frequently changing user passwords is a good general security practice that ensures intruders cannot enter into the IT infrastructure. It is a best practice to change your passwords every 30 to 90 days.

Administrators must identify and review all password change events to ensure users are changing passwords at least every 90 days. For example, Windows platforms generate events with the ID of 627 and 628 for password change attempts.

Reports and Alerts

Use the following link or reference to see the 164.308(a)(5)(ii)(D) reports and alerts: 164.308(a)(5)(ii)(D) - Password Management (Addressable).

164.308(a)(6) Security Incident Procedures

Implement policies and procedures to address security incidents.

Implementation Specification	Description
164.308(a)(6)(ii)	**Response and Reporting (Required)** Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

164.308(a)(6)(ii) - Response and Reporting (Required)

Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

Illustrative Controls and TIBCO LogLogic Solution

Ensure that security techniques and related management procedures are used to authorize access and control information flows from and to networks such as Intrusion Detection.

The security incident management system must provide for adequate audit trail facilities that allow tracking, analyzing, and determining the root cause of all reported problems considering:

- All associated configuration items
- Outstanding problems and incidents
- Known and suspected errors
- Managing problems and incidents addresses how an organization identifies documents and responds to events that fall outside of normal operations. You must maintain a complete and accurate audit trail for network devices, servers and applications. This enables you to address how your business identify root causes of issues that may introduce inaccuracy in healthcare reporting. Also, your problem management system must provide for adequate audit trail facilities that allow tracing from incident to underlying cause.
- To satisfy this requirement, administrators must periodically review IDS logs to ensure the IDS tools are fully utilized. In addition, administrators must ensure all network devices, servers, and applications are properly configured to log to a centralized server. Administrators must also periodically review logging status to ensure these devices, servers and applications are logging correctly.
- By alerting on any failures that occur, administrators can respond rapidly to potential problems and incidents that might affect availability, security, or performance. Real-time data monitoring and reporting capabilities reduce time to repair after incidents, reducing costs, and improving application availability.

Reports and Alerts

Use the following link or reference to see the 164.308(a)(6)(ii) reports and alerts: 164.308(a)(6)(ii) - Response and Reporting (Required).

164.308(a)(7) Contingency Plan

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 health information.

Implementation Specification	Description
164.308(a)(7)(ii)(A)	**Data Backup Plan (Required)** Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

Implementation Specification	Description
164.308(a)(7)(ii)(B)	**Disaster Recovery Plan (Required)** Establish (and implement as needed) procedures to restore any loss of data.
164.308(a)(7)(ii)(C)	**Emergency Mode Operational Plan (Required)** Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.
164.308(a)(7)(ii)(D)	**Testing and Revision Procedures (Addressable)** Implement procedures for periodic testing and revision of contingency plans.

164.308(a)(7)(ii)(A) - Data Backup Plan (Required)

Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

Reports and Alerts

Use the following link or reference to see the 164.308(a)(7)(ii)(A) reports and alerts: 164.308(a)(7)(ii)(A) - Data Backup Plan (Required).

164.308(a)(7)(ii)(B) - Disaster Recovery Plan (Required)

Establish (and implement as needed) procedures to restore any loss of data.

Illustrative Controls and TIBCO LogLogic Solution

Organizations must develop a framework for IT continuity to support enterprise-wide business continuity management with a consistent process. The objective of the framework is to assist in determining the required resilience of the infrastructure and to drive the development of disaster recovery and IT contingency plans. The framework should address the organizational structure for continuity management, covering the roles, tasks and responsibilities of internal and external service providers, their management and their customers, and the rules and structures to document, test and execute the disaster recovery and IT contingency plans. The plan should also address items such as the identification of critical resources, the monitoring and reporting of the availability of critical resources, alternative processing, and the principles of backup and recovery.

Organizations must have procedures in place to back up data and programs based on IT and user requirements. Organizations must define and implement procedures for backup and restoration of systems, data and documentation in line with business requirements and the continuity plan. Verify compliance with the backup procedures, and verify the ability to and time required for successful and complete restoration. Test backup media and the restoration process.

To satisfy this Implementation specification, administrators must back up data on a regular basis. In addition, administrators must review backup logs periodically to ensure backups are performed successfully. Backup logs must be reviewed periodically to ensure backup and restore are performed successfully on a regular basis.

TIBCO LogLogic directly supports this Implementation specification since TIBCO LogLogic reports and alerts are capable of extracting system records that validate when and if a backup was performed and if the backup is an exact copy of the original. TIBCO LogLogic can monitor systems to ensure that data backups are successfully accomplished on time and so that data restores are possible. They can also

monitor and alert you when a data restore is completed successfully or unsuccessfully, so that the integrity of backup data is retained if you need to exercise a disaster recovery plan.

Reports and Alerts

Use the following link or reference to see the 164.308(a)(7)(ii)(B) reports and alerts: 164.308(a)(7)(ii)(B) - Disaster Recovery Plan (Required).

164.308(a)(7)(ii)(C) - Emergency Mode Operational Plan (Required)

Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

Illustrative Controls and TIBCO LogLogic Solution

It is inevitable that accounts must be created for emergency mode access. These accounts may be required for vendors so they can perform remote troubleshooting as well as maintenance of the equipment in the IT infrastructure. Care must be taken to ensure that these vendors only have access during maintenance hours and when personnel are available to monitor the process.

Administrators must identify all access to ensure vendors are only logging in during maintenance hours. Administrators must also review access to the IT infrastructure to ensure no access is performed during unauthorized hours.

Reports and Alerts

Use the following link or reference to see the 164.308(a)(7)(ii)(C) reports and alerts: 164.308(a)(7)(ii)(C) - Emergency Mode Operational Plan (Required).

164.308(a)(7)(ii)(D) - Testing and Revision Procedures (Addressable)

Implement procedures for periodic testing and revision of contingency plans.

Illustrative Controls and TIBCO LogLogic Solution

Test the IT continuity plan on a regular basis to ensure that IT systems can be effectively recovered, shortcomings are addressed and the plan remains relevant. This requires careful preparation, documentation, reporting test results and, according to the results, implementing an action plan. Consider the extent of testing recovery of single applications to integrated testing scenarios to end-to-end testing and integrated vendor testing.

Organizations must have procedures in place to back up data and programs based on IT and user requirements. To satisfy this control objective, administrators must back up data on a regular basis. In addition, administrators must review backup logs periodically to ensure backups are performed successfully. Backup logs must be reviewed periodically to ensure backup and restore are performed successfully on a regular basis. Organizations must review backup logs periodically to ensure backup and restore are performed successfully on a regular basis.

Reports and Alerts

Use the following link or reference to see the 164.308(a)(7)(ii)(D) reports and alerts: 164.308(a)(7)(ii)(D) - Testing and Revision Procedures (Addressable).

164.312(a)(1) Access Control

Implement 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.

Implementation Specification	Description
164.312(a)(2)(i)	**Unique User Identification (Required)** Assign a unique name and/or number for identifying and tracking user identity.
164.312(a)(2)(ii)	**Emergency Access Procedure (Required)** Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.
164.312(a)(2)(iii)	**Automatic Logoff (Addressable)** Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

164.312(a)(2)(i) – Unique User Identification (Required)

Assign a unique name and/or number for identifying and tracking user identity.

Illustrative Controls and TIBCO LogLogic Solution

All users (internal, external and temporary) and their activity on IT systems (business application, system operation, development and maintenance) must be uniquely identifiable. Ensuring all users have uniquely identifiable IDs ensures that accurate and complete audit trails can be maintained. Deficiencies in this area can significantly impact accountability. For example, users logging in using shared IDs can modify healthcare records. This can prevent future audits to identify who has modified the data.

To satisfy this requirement, administrators must ensure that not all logins are shared. Administrators must review the ID list to identify IDs that might be a generic ID and question who is using it and why it is there. Administrators can review the time and sources of the logins to determine whether they overlap. If the time overlap and sources are different, it indicates a shared (or generic) ID. Administrators must also validate that attempts to gain unauthorized access to healthcare reporting systems and subsystems are logged and are followed up on a timely basis.

Reports and Alerts

Use the following link or reference to see the 164.312(a)(2)(i) reports and alerts: 164.312(a)(2)(i) – Unique User Identification (Required).

164.312(a)(2)(ii) - Emergency Access Procedure (Required)

Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

Illustrative Controls and TIBCO LogLogic Solution

Accounts must be created for emergency mode access. These accounts may be required for vendors so they can perform remote troubleshooting as well as maintenance of the equipment in the IT

infrastructure. Care must be taken to ensure that these vendors only have access during maintenance hours and when personnel are available to monitor the process.

Administrators must identify all access to ensure vendors are only logging in during maintenance hours. Administrators must also review access to the IT infrastructure to ensure no access is performed during unauthorized hours.

Reports and Alerts

Use the following link or reference to see the 164.312(a)(2)(ii) reports and alerts: 164.312(a)(2)(iii) - Automatic Logoff (Addressable).

164.312(a)(2)(iii) - Automatic Logoff (Addressable)

Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

Illustrative Controls and TIBCO LogLogic Solution

TIBCO LogLogic reports and alerts should be used to ensure that systems are configured to terminate an electronic session after a predetermined time of inactivity. TIBCO LogLogic reports contain information about configuration changes that impact logoffs due to system inactivity. TIBCO LogLogic alerts can trigger a response by the system administrator when system inactivity logout configurations are altered or disabled. Group policies that govern logout inactivity configurations can also be reviewed or trigger an alerts when they are altered or disabled so this Implementation specification is enforced.

Reports and Alerts

Use the following link or reference to see the 164.312(a)(2)(iii) reports and alerts: 164.312(a)(2)(iii) - Automatic Logoff (Addressable).

164.312(b) Audit Controls (Required)

Implement hardware, software, and procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

Illustrative Controls and TIBCO LogLogic Solution

Audit trails maintain a record of system activity both by system and application processes and by user activity of systems and applications. In conjunction with appropriate tools and procedures, audit trails can assist in detecting security violations, performance problems, and flaws in applications.

The auditor can obtain valuable information about activity on a computer system from the audit trail. Audit trails improve the auditability of the computer system. Organizations must maintain a complete and accurate audit trail for network devices, servers, and applications. This enables organizations to address how businesses identify root causes of issues that might introduce inaccuracy in healthcare reporting. Also, problem management system must provide for adequate audit trail facilities that allow tracing from incident to underlying cause.

IT security administration must monitor and log security activity, and identify security violations to report to senior management. This control directly addresses the Implementation specification for audit controls over electronic protected health information systems and networks.

To satisfy this control objective, administrators must ensure all network devices, servers, and applications are properly configured to log to a centralized server. Administrators must also periodically review logging status to ensure these devices, servers and applications are logging correctly.

The TIBCO LogLogic® Log Management Intelligence (LMI) automatically records the event date and time, event status (success or failure), event origin (log source IP address) and event type (firewall connection, access or authentication, IDS, e-mail, or web access) for every single event. In addition,

TIBCO LogLogic identifies all users, system components, or resources within the events to help administrator correctly analyze the events.

Reports and Alerts

Use the following link or reference to see the 164.312(b) reports and alerts: 164.312(b) Audit Controls (Required).

164.312(d) Person or Entity Authentication (Required)

Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

Illustrative Controls and TIBCO LogLogic Solution

Authentication systems identify persons or entities seeking access to electronic protected health information by challenging the person or entity for something they know, something they are or something they possess. By using these methods, a person or entity is “authenticated” as the one that the individual or entity claimed to be. TIBCO LogLogic is used to capture system activity and log records to detail system, file or facility access events, as well as authentication system configuration changes so covered entities can ensure their authentication procedures safeguard against unauthorized access to electronic protected health information systems, files and facilities.

To satisfy this HIPAA standard requirement, administrators must assess the authentication mechanisms used to validate user credentials (new and existing) for electronic protected health information systems to support the validity of transactions. Server and application activities must be monitored for locked-out and enabled accounts as they can represent malicious activities. Administrators must monitor and verify all user access to programs and data, and review access to ensure there is segregation of duties as well as all access privileges are properly assigned and approved.

Reports and Alerts

Use the following link or reference to see the 164.312(d) reports and alerts: 164.312(d) Person or Entity Authentication (Required).

164.312(c)(1) Integrity

Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

Implementation Specification	Description
164.312(c)(2)	**Mechanism to Authenticate Electronic Protected Health Information (Addressable)** Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

164.312(c)(2) - Mechanism to Authenticate Electronic Protected Health Information (Addressable)

Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

Illustrative Controls and TIBCO LogLogic Solution

A logging and monitoring function enables the early detection of unusual or abnormal activities. Administrators must ensure that IT security implementation is tested and monitored proactively.

IT security should be routinely reaccredited to ensure the approved security level is maintained. IT security administration must monitor and log security activity, and identify security violations to report to senior management. This control directly addresses the Implementation specification for audit controls over electronic protected health information systems and networks.

To satisfy this requirement, administrators must review the user access logs on a regular basis for any access violations or unusual activity. Administrators must routinely review reports that show user access to servers that store, process or transmit electronic protected health information. Review of these reports must be shown to auditors to satisfy this requirement.

The TIBCO LogLogic Compliance Suite captures the activities on information systems and communication devices across the entity's enterprise to allow entities to oversee the protection of electronic protected health information. Activities that increase risk or potentially impact the integrity and authenticity of electronic protected health information are highlighted in custom reports and alerts so the security posture of the enterprise can be maintained. Because of the breadth of solutions and devices that TIBCO LogLogic interfaces with, data can be cross referenced to provide a corroborative method of analyzing threats to the integrity, confidentiality and availability of electronic protected health information.

Reports and Alerts

Use the following link or reference to see the 164.312(c)(2) reports and alerts: 164.312(c)(2) - Mechanism to Authenticate Electronic Protected Health Information (Addressable).

TIBCO LogLogic Reports and Alerts for HIPAA

TIBCO LogLogic Reports for HIPAA

All TIBCO LogLogic reports can be used to monitor regular user activity, as well as the activity and results of system and network administrators.

Serial Number	TIBCO LogLogic Report	Description
1	HIPAA: Accepted VPN Connections - RADIUS	Displays all users connected to the internal network through the RADIUS VPN.
2	HIPAA: Account Activities on UNIX Servers	Displays all accounts activities on UNIX servers to ensure authorized and appropriate access.
3	HIPAA: Account Activities on Windows Servers	Displays all accounts activities on Windows servers to ensure authorized and appropriate access.
4	HIPAA: Accounts Changed on NetApp Filer	Displays all accounts changed on NetApp Filer to ensure authorized and appropriate access.
5	HIPAA: Accounts Changed on TIBCO Administrator	Displays all accounts changed on TIBCO Administrator to ensure authorized and appropriate access.
6	HIPAA: Accounts Changed on TIBCO ActiveMatrix Administrator	Displays all accounts changed on TIBCO ActiveMatrix Administrator to ensure authorized and appropriate access.
7	HIPAA: Accounts Changed on UNIX Servers	Displays all accounts changed on UNIX servers to ensure authorized and appropriate access.
8	HIPAA: Accounts Changed on Windows Servers	Displays all accounts changed on Windows servers to ensure authorized and appropriate access.
9	HIPAA: Accounts Created on NetApp Filer	Displays all accounts created on NetApp Filer to ensure authorized and appropriate access.
10	HIPAA: Accounts Created on NetApp Filer Audit	Displays all accounts created on NetApp Filer Audit to ensure authorized and appropriate access.
11	HIPAA: Accounts Created on Sidewinder	Displays all accounts created on Sidewinder to ensure authorized and appropriate access.
12	HIPAA: Accounts Created on Symantec Endpoint Protection	Displays all accounts created on Symantec Endpoint Protection to ensure authorized and appropriate access.

Serial Number	TIBCO LogLogic Report	Description
13	HIPAA: Accounts Created on TIBCO Administrator	Displays all accounts created on TIBCO Administrator to ensure authorized and appropriate access.
14	HIPAA: Accounts Created on TIBCO ActiveMatrix Administrator	Displays all accounts created on TIBCO ActiveMatrix Administrator to ensure authorized and appropriate access.
15	HIPAA: Accounts Created on UNIX Servers	Displays all accounts created on UNIX servers to ensure authorized and appropriate access.
16	HIPAA: Accounts Created on Windows Servers	Displays all accounts created on Windows servers to ensure authorized and appropriate access.
17	HIPAA: Accounts Deleted on NetApp Filer	Displays all accounts deleted on NetApp Filer to ensure authorized and appropriate access.
18	HIPAA: Accounts Deleted on NetApp Filer Audit	Displays all accounts deleted on NetApp Filer Audit to ensure authorized and appropriate access.
19	HIPAA: Accounts Deleted on Sidewinder	Displays all accounts deleted on Sidewinder to ensure authorized and appropriate access.
20	HIPAA: Accounts Deleted on Symantec Endpoint Protection	Displays all accounts deleted on Symantec Endpoint Protection to ensure authorized and appropriate access.
21	HIPAA: Accounts Deleted on TIBCO Administrator	Displays all accounts deleted on TIBCO Administrator to ensure authorized and appropriate access.
22	HIPAA: Accounts Deleted on TIBCO ActiveMatrix Administrator	Displays all accounts deleted on TIBCO ActiveMatrix Administrator to ensure authorized and appropriate access.
23	HIPAA: Accounts Deleted on UNIX Servers	Displays all accounts deleted on UNIX servers to ensure authorized and appropriate access.
24	HIPAA: Accounts Deleted on Windows Servers	Displays all accounts deleted on Windows servers to ensure authorized and appropriate access.
25	HIPAA: Active Directory Sys tem Changes	Displays changes made within Active Directory.
26	HIPAA: Administrators Activities on Servers	Displays the latest activities performed by administrators and root users to ensure appropriate access.
27	HIPAA: Applications Under Attack	Displays all applications under attack as well as the attack signatures.
28	HIPAA: Applications Under Attack - Cisco IOS	Displays all applications under attack as well as the attack signatures by Cisco IOS.

Serial Number	TIBCO LogLogic Report	Description
29	HIPAA: Applications Under Attack - FireEye MPS	Displays all applications under attack as well as the attack signatures by FireEye MPS.
30	HIPAA: Applications Under Attack - ISS SiteProtector	Displays all applications under attack as well as the attack signatures by ISS SiteProtector.
31	HIPAA: Applications Under Attack - SiteProtector	Displays all applications under attack as well as the attack signatures by SiteProtector.
32	HIPAA: Applications Under Attack - Sourcefire Defense Center	Displays all applications under attack as well as the attack signatures by Sourcefire Defense Center.
33	HIPAA: Attacks Detected	Displays all IDS attacks detected against servers and applications.
34	HIPAA: Attacks Detected - Cisco IOS	Displays all IDS attacks detected against servers and applications by Cisco IOS.
35	HIPAA: Attacks Detected - HIPS	Displays all IPS attacks detected against servers and applications.
36	HIPAA: Attacks Detected - ISS SiteProtector	Displays all IDS attacks detected against servers and applications by ISS SiteProtector.
37	HIPAA: Attacks Detected - SiteProtector	Displays all IDS attacks detected against servers and applications by SiteProtector
38	HIPAA: Attacks Detected - Sourcefire Defense Center	Displays all IDS attacks detected against servers and applications by Sourcefire Defense Center
39	HIPAA: Attack Origins	Displays the sources that have initiated the most attacks.
40	HIPAA: Attack Origins - Cisco IOS	Displays the sources that have initiated the most attacks by Cisco IOS.
41	HIPAA: Attack Origins - HIPS	Displays the sources that have initiated the most attacks.
42	HIPAA: Attack Origins - ISS SiteProtector	Displays the sources that have initiated the most attacks by ISS SiteProtector.
43	HIPAA: Attack Origins - SiteProtector	Displays the sources that have initiated the most attacks by SiteProtector
44	HIPAA: Attack Origins - Sourcefire Defense Center	Displays the sources that have initiated the most attacks by Sourcefire Defense Center
45	HIPAA: Check Point Management Station Login	Displays all login events to the Check Point management station.

Serial Number	TIBCO LogLogic Report	Description
46	HIPAA: Check Point Management Station Logout	Displays all logoff events to the Check Point management station.
47	HIPAA: Check Point Object Activity	Displays all creation, deletion, and modification of Check Point objects.
48	HIPAA: Check Point Configuration Changes	Displays all Check Point audit events related to configuration changes.
49	HIPAA: Cisco ESA: Attacks by Event ID	Displays Cisco ESA attacks by Event ID.
50	HIPAA: Cisco ESA: Attacks Detected	Displays attacks detected by Cisco ESA.
51	HIPAA: Cisco ESA: Attacks by Threat Name	Displays Cisco ESA attacks by threat name.
52	HIPAA: Cisco ESA: Scans	Displays scans using Cisco ESA.
53	HIPAA: Cisco ESA: Updated	Displays updates to Cisco ESA.
54	HIPAA: Cisco ISE, ACS Accounts Created	Displays all accounts created on Cisco ISE and Cisco SecureACS to ensure authorized and appropriate access.
55	HIPAA: Cisco ISE, ACS Accounts Removed	Displays all accounts removed on Cisco ISE and Cisco SecureACS to ensure authorized and appropriate access.
56	HIPAA: Cisco ISE, ACS Configuration Changes	Displays Cisco ISE and Cisco SecureACS configuration changes.
57	HIPAA: Cisco ISE, ACS Password Changes	Displays all password change activities on Cisco ISE and Cisco SecureACS to ensure authorized and appropriate access.
58	HIPAA: Cisco PIX, ASA, FWSM Failover Disabled	Displays all logs related to disabling Cisco PIX, ASA, and FWSM failover capability.
59	HIPAA: Cisco PIX, ASA, FWSM Failover Performed	Displays all logs related to performing a Cisco PIX, ASA, and FWSM failover.
60	HIPAA: Cisco PIX, ASA, FWSM Restarted	Displays all Cisco PIX, ASA, or FWSM restart activities to detect unusual activities.
61	HIPAA: Cisco PIX, ASA, FWSM Routing Failure	Displays all Cisco PIX, ASA, and FWSM routing error messages.
62	HIPAA: Cisco PIX, ASA, FW SM Policy Changed	Displays all configuration changes made to the Cisco PIX, ASA, and FWSM devices.

Serial Number	TIBCO LogLogic Report	Description
63	HIPAA: Cisco Routers and Switches Restart	Displays all Cisco routers and switches restart activities to detect unusual activities.
64	HIPAA: Cisco Switch Policy Changes	Displays all configuration changes to the Cisco router and switch policies.
65	HIPAA: Creation and Deletion of System Level Objects: DB2 Database	Displays DB2 database events related to creation and deletion of system-level objects.
66	HIPAA: Creation and Deleti on of System Level Objects: Oracle	Displays Oracle database events related to creation and deletion of system-level objects.
67	HIPAA: Creation and Deletion of System Level Objects: SQL Server	Displays Microsoft SQL Server events related to creation and deletion of system-level objects.
68	HIPAA: Creation and Deletion of System Level Objects: Windows	Displays all Windows events related to creation and deletion of system-level objects.
69	HIPAA: DB2 Database Configuration Changes	Displays DB2 database configuration changes.
70	HIPAA: DB2 Database Failed Logins	Displays all failed login attempts to review any access violations or unusual activity.
71	HIPAA: DB2 Database Successful Logins	Displays successful DB2 database logins.
72	HIPAA: DB2 Database User Additions and Deletions	Displays IBM DB2 Database events related to creation and deletion of database users.
73	HIPAA: Denied VPN Connections - RADIUS	Displays all users denied access to the internal network by the RADIUS VPN.
74	HIPAA: DHCP Granted/ Renewed Activities on Microsoft DHCP	Displays all DHCP Granted or Renewed Activities on Microsoft DHCP Server.
75	HIPAA: DHCP Granted/ Renewed Activities on VMware vShield	Displays all DHCP Granted or Renewed Activities on VMware vShield Edge.
76	HIPAA: DNS Server Error	Displays all events when DNS Server has errors.
77	HIPAA: Escalated Privilege Activities on Servers	Displays all privilege escalation activities performed on servers to ensure appropriate access.

Serial Number	TIBCO LogLogic Report	Description
78	HIPAA: ESX Accounts Activities	Displays all accounts activities on VMware ESX servers to ensure authorized and appropriate access.
79	HIPAA: ESX Accounts Created	Displays all accounts created on VMware ESX servers to ensure authorized and appropriate access.
80	HIPAA: ESX Accounts Deleted	Displays all accounts deleted on VMware ESX servers to ensure authorized and appropriate access.
81	HIPAA: ESX Failed Logins	Failed VMware ESX logins for known user.
82	HIPAA: ESX Group Activities	Displays all group activities on VMware ESX servers to ensure authorized and appropriate access.
83	HIPAA: ESX Kernel log daemon terminating	Displays all VMware ESX Kernel log daemon terminating.
84	HIPAA: ESX Kernel logging Stop	Displays all VMware ESX Kernel logging stops.
85	HIPAA: ESX Logins Failed Unknown User	Failed VMware ESX logins for unknown user.
86	HIPAA: ESX Logins Succeeded	Displays successful logins to VMware ESX to ensure only authorized personnel have access.
87	HIPAA: ESX Syslogd Restart	Displays all VMware ESX syslogd restarts.
88	HIPAA: F5 BIG-IP TMOS Login Failed	Displays all F5 BIG-IP TMOS login events which have failed.
89	HIPAA: F5 BIG-IP TMOS Login Successful	Displays all F5 BIG-IP TMOS login events which have succeeded.
90	HIPAA: F5 BIG-IP TMOS Password Changes	Displays all password change activities on F5 BIG-IP TMOS to ensure authorized and appropriate access.
91	HIPAA: F5 BIG-IP TMOS Restarted	Displays all events when the F5 BIG-IP TMOS has been restarted.
92	HIPAA: Failed Logins	Displays all failed login attempts to review any access violations or unusual activity.
93	HIPAA: Files Accessed on NetApp Filer Audit	Displays all files accessed on NetApp Filer Audit to ensure appropriate access.
94	HIPAA: Files Accessed on Servers	Displays all files accessed on servers to ensure appropriate access.

Serial Number	TIBCO LogLogic Report	Description
95	HIPAA: Files Accessed through Juniper SSL VPN (Secure Access)	Displays all files accessed through Juniper SSL VPN (Secure Access).
96	HIPAA: Files Accessed through PANOS	Displays all files accessed through Palo Alto Networks.
97	HIPAA: Files Accessed through Pulse Connect Secure	Displays all files accessed through Pulse Connect Secure.
98	HIPAA: FireEye MPS: Attacks Detected	Displays attacks detected by FireEye MPS.
99	HIPAA: FireEye MPS: Attacks by Event ID	Displays FireEye MPS attacks by Event ID.
100	HIPAA: FireEye MPS: Attacks by Threat Name	Displays FireEye MPS attacks by threat name.
101	HIPAA: Firewall Connections Accepted - Check Point	Displays all traffic passing through the Check Point firewall.
102	HIPAA: Firewall Connections Accepted - Cisco ASA	Displays all traffic passing through the Cisco ASA firewall.
103	HIPAA: Firewall Connections Accepted - Cisco FWSM	Displays all traffic passing through the Cisco FWSM firewall.
104	HIPAA: Firewall Connections Accepted - Cisco IOS	Displays all traffic passing through the Cisco IOS firewall.
105	HIPAA: Firewall Connections Accepted - Cisco Netflow	Displays all traffic passing through the Cisco Netflow.
106	HIPAA: Firewall Connections Accepted - Cisco NXOS	Displays all traffic passing through the Cisco NXOS device.
107	HIPAA: Firewall Connections Accepted - Cisco PIX	Displays all traffic passing through the Cisco PIX firewall.
108	HIPAA: Firewall Connections Accepted - F5 BIG-IP TMOS	Displays all traffic passing through the F5 BIG-IP TMOS device.

Serial Number	TIBCO LogLogic Report	Description
109	HIPAA: Firewall Connections Accepted - Fortinet	Displays all traffic passing through the Fortinet firewall.
110	HIPAA: Firewall Connections Accepted - Juniper Firewall	Displays all traffic passing through the Juniper Firewall.
111	HIPAA: Firewall Connections Accepted - Juniper JunOS	Displays all traffic passing through the Juniper JunOS firewall.
112	HIPAA: Firewall Connections Accepted - Juniper RT Flow	Displays all traffic passing through the Juniper RT Flow.
113	HIPAA: Firewall Connections Accepted - Nortel	Displays all traffic passing through the Nortel firewall.
114	HIPAA: Firewall Connections Accepted - PANOS	Displays all traffic passing through the Palo Alto Networks firewall.
115	HIPAA: Firewall Connections Accepted - Sidewinder	Displays all traffic passing through the Sidewinder firewall.
116	HIPAA: Firewall Connections Accepted - VMware vShield	Displays all traffic passing through the VMware vShield device.
117	HIPAA: Firewall Connections Denied - Check Point	Displays the applications that have been denied access the most by the Check Point devices.
118	HIPAA: Firewall Connections Denied - Cisco ASA	Displays the applications that have been denied access the most by the Cisco ASA devices.
119	HIPAA: Firewall Connections Denied - Cisco FWSM	Displays the applications that have been denied access the most by the Cisco FWSM devices.
120	HIPAA: Firewall Connections Denied - Cisco IOS	Displays the applications that have been denied access the most by the Cisco IOS.
121	HIPAA: Firewall Connections Denied - Cisco NXOS	Displays the applications that have been denied access the most by the Cisco NXOS devices.

Serial Number	TIBCO LogLogic Report	Description
122	HIPAA: Firewall Connections Denied - Cisco PIX	Displays the applications that have been denied access the most by the Cisco PIX devices.
123	HIPAA: Firewall Connections Denied - Cisco Router	Displays the applications that have been denied access the most by the Cisco Router.
124	HIPAA: Firewall Connections Denied - F5 BIG-IP TMOS	Displays the applications that have been denied access the most by the F5 BIG-IP TMOS.
125	HIPAA: Firewall Connections Denied - Fortinet	Displays the applications that have been denied access the most by the Fortinet devices.
126	HIPAA: Firewall Connections Denied - Juniper Firewall	Displays the applications that have been denied access the most by the Juniper Firewall.
127	HIPAA: Firewall Connections Denied - Juniper JunOS	Displays the applications that have been denied access the most by the Juniper JunOS.
128	HIPAA: Firewall Connections Denied - Juniper RT Flow	Displays the applications that have been denied access the most by the Juniper RT Flow.
129	HIPAA: Firewall Connections Denied - Nortel	Displays the applications that have been denied access the most by the Nortel devices.
130	HIPAA: Firewall Connections Denied - PANOS	Displays the applications that have been denied access the most by the Palo Alto Networks devices.
131	HIPAA: Firewall Connections Denied - Sidewinder	Displays the applications that have been denied access the most by the Sidewinder.
132	HIPAA: Firewall Connections Denied - VMware vShield	Displays the applications that have been denied access the most by the VMware vShield.
133	HIPAA: Firewall Traffic Considered Risky - Check Point	Displays Check Point allowed firewall traffic that is considered risky.
134	HIPAA: Firewall Traffic Considered Risky - Cisco ASA	Displays Cisco ASA allowed firewall traffic that is considered risky.

Serial Number	TIBCO LogLogic Report	Description
135	HIPAA: Firewall Traffic Considered Risky - Cisco FWSM	Displays Cisco FWSM allowed firewall traffic that is considered risky.
136	HIPAA: Firewall Traffic Considered Risky - Cisco IOS	Displays Cisco IOS allowed firewall traffic that is considered risky.
137	HIPAA: Firewall Traffic Considered Risky - Cisco Netflow	Displays Cisco Netflow allowed firewall traffic that is considered risky.
138	HIPAA: Firewall Traffic Considered Risky - Cisco PIX	Displays Cisco PIX allowed firewall traffic that is considered risky.
139	HIPAA: Firewall Traffic Considered Risky - F5 BIG-IP TMOS	Displays F5 BIG-IP TMOS allowed firewall traffic that is considered risky.
140	HIPAA: Firewall Traffic Considered Risky - Fortinet	Displays Fortinet allowed firewall traffic that is considered risky.
141	HIPAA: Firewall Traffic Considered Risky - Juniper Firewall	Displays Juniper Firewall allowed firewall traffic that is considered risky.
142	HIPAA: Firewall Traffic Considered Risky - Juniper JunOS	Displays Juniper JunOS allowed firewall traffic that is considered risky.
143	HIPAA: Firewall Traffic Considered Risky - Juniper RT Flow	Displays Juniper RT Flow allowed firewall traffic that is considered risky.
144	HIPAA: Firewall Traffic Considered Risky - Nortel	Displays Nortel allowed firewall traffic that is considered risky.
145	HIPAA: Firewall Traffic Considered Risky - PANOS	Displays Palo Alto Networks allowed firewall traffic that is considered risky.
146	HIPAA: Firewall Traffic Considered Risky - Sidewinder	Displays Sidewinder allowed firewall traffic that is considered risky.
147	HIPAA: Firewall Traffic Considered Risky - VMware vShield	Displays VMware vShield Edge allowed firewall traffic that is considered risky.
148	HIPAA: FortiOS: Attacks by Event ID	Displays FortiOS attacks by Event ID.

Serial Number	TIBCO LogLogic Report	Description
149	HIPAA: FortiOS: Attacks by Threat Name	Displays FortiOS attacks by threat name.
150	HIPAA: FortiOS: Attacks Detected	Displays attacks detected by FortiOS.
151	HIPAA: FortiOS DLP Attacks Detected	Displays all DLP attacks detected by FortiOS.
152	HIPAA: Group Activities on UNIX Servers	Displays all group activities on UNIX servers to ensure authorized and appropriate access.
153	HIPAA: Group Activities on Windows Servers	Displays all group activities on Windows servers to ensure authorized and appropriate access.
154	HIPAA: Guardium SQL Guard Audit Configuration Changes	Displays all configuration changes on the Guardium SQL Guard Audit database.
155	HIPAA: Guardium SQL Guard Audit Data Access	Displays all select statements made on Guardium SQL Audit Server.
156	HIPAA: Guardium SQL Guard Audit Logins	Displays all login attempts to the Guardium SQL Server Audit database.
157	HIPAA: Guardium SQL Guard Configuration Changes	Displays all configuration changes on the Guardium SQL Guard database.
158	HIPAA: Guardium SQL Guard Data Access	Displays all select statements made on Guardium SQL Server.
159	HIPAA: Guardium SQL Guard Logins	Displays all login attempts to the Guardium SQL Server database.
160	HIPAA: Group Activities on NetApp Filer Audit	Displays all group activities on NetApp Filer Audit to ensure authorized and appropriate access.
161	HIPAA: Group Activities on Symantec Endpoint Protection	Displays all group activities on Symantec Endpoint Protection to ensure authorized and appropriate access.
162	HIPAA: Group Activities on TIBCO ActiveMatrix Administrator	Displays all group activities on TIBCO ActiveMatrix Administrator to ensure authorized and appropriate access.
163	HIPAA: HP NonStop Audit Configuration Changes	Displays all audit configuration changes on HP NonStop.
164	HIPAA: HP NonStop Audit Login Failed	Displays all HP NonStop Audit login events which have failed.

Serial Number	TIBCO LogLogic Report	Description
165	HIPAA: HP NonStop Audit Login Successful	Displays all HP NonStop Audit login events which have succeeded.
166	HIPAA: HP NonStop Audit Object Changes	Displays HP NonStop Audit events related to object changes.
167	HIPAA: HP NonStop Audit Permissions Changed	Displays all permission modification activities on HP NonStop Audit to ensure authorized access.
168	HIPAA: i5/ OS DST Password Reset	Displays i5/OS events related to the reset of the DST (Dedicated Service Tools) password.
169	HIPAA: i5/OS Files Accessed	Lists all events when a user gains access an i5/OS file.
170	HIPAA: i5/ OS Network User Login Fail ed	Lists all events when a network user was denied access into the i5/OS.
171	HIPAA: i5/ OS Network User Login Successful	Lists all events when a network user successfully logs into the i5/OS.
172	HIPAA: i5/ OS Network User Profile Creation	Displays i5/OS events when a network user profile has been created.
173	HIPAA: i5/ OS Network User Profile Deletion	Displays i5/OS events when a network user profile has been deleted.
174	HIPAA: i5/ OS Network User Profile Modified	Displays i5/OS events when a network user profile has been modified.
175	HIPAA: i5/OS Object Permissions Modified	Displays all permission modification activities on i5/OS to ensure authorized access.
176	HIPAA: i5/OS Restarted	Lists all events when the i5/OS has been restarted.
177	HIPAA: i5/ OS Service Started	Lists all events when a user starts a service on the i5/OS.
178	HIPAA: i5/ OS User Login Failed	Lists all events when a user was denied access into the i5/OS.
179	HIPAA: i5/OS User Login Successful	Lists all events when a user successfully logs into the i5/OS.
180	HIPAA: i5/OS User Profile Creation	Displays i5/OS events when a user profile has been created.

Serial Number	TIBCO LogLogic Report	Description
181	HIPAA: i5/OS User Profile Modifications	Displays i5/OS events when a user profile has been modified.
182	HIPAA: Juniper Firewall HA State Changed	Displays all Juniper Firewall fail-over state change events.
183	HIPAA: Juniper Firewall Policy Changed	Displays all configuration changes to the Juniper Firewall policies.
184	HIPAA: Juniper Firewall Policy Out of Sync	Displays events that indicate the Juniper Firewall's HA policies are out of sync.
185	HIPAA: Juniper Firewall Reset Accepted	Displays events that indicate the Juniper Firewall has been reset to its factory default state.
186	HIPAA: Juniper Firewall Reset Imminent	Displays events that indicate the Juniper Firewall is reset to its factory default state.
187	HIPAA: Juniper SSL VPN (Secure Access) Policy Changed	Displays all configuration changes to the Juniper SSL VPN (Secure Access) policies.
188	HIPAA: Juniper SSL VPN (Secure Access) Successful Logins by IP	Displays all successful Juniper SSL VPN (Secure Access) logins based on IP address.
189	HIPAA: Juniper SSL VPN (Secure Access) Successful Logins by User	Displays all successful Juniper SSL VPN (Secure Access) logins based on user.
190	HIPAA: Juniper SSL VPN Successful Logins by IP	Displays all successful Juniper SSL VPN logins based on IP address.
191	HIPAA: Juniper SSL VPN Successful Logins by U ser	Displays all successful Juniper SSL VPN logins based on user.
192	HIPAA: Logins by Authentication Type	Displays all logins categorized by the authentication type.
193	HIPAA: LogLogic Disk Full	Displays events that indicate the LogLogic appliance's disk is near full.
194	HIPAA: LogLogic DSM Configuration Changes	Displays all configuration changes on the LogLogic DSM database.
195	HIPAA: LogLogic DSM Data Access	Displays all select statements made on LogLogic DSM database.
196	HIPAA: LogLogic DSM Logins	Displays all login attempts to the LogLogic DSM database.

Serial Number	TIBCO LogLogic Report	Description
197	HIPAA: LogLogic File Retrieval Errors	Displays all errors while retrieving log files from devices, servers and applications.
198	HIPAA: LogLogic HA State Changed	Displays all LogLogic appliance failover state change events.
199	HIPAA: LogLogic Management Center Account Activities	Displays all accounts activities on LogLogic management center to ensure authorized and appropriate access.
200	HIPAA: LogLogic Management Center Login	Displays all login events to the LogLogic management center.
201	HIPAA: LogLogic Management Center Password Changes	Displays all password change activities on LogLogic management center to ensure authorized and appropriate access.
202	HIPAA: LogLogic Management Center Upgrade Success	Displays all successful events related to the system's upgrade.
203	HIPAA: LogLogic Universal Collector Configuration Changes	Displays LogLogic universal collector configuration changes.
204	HIPAA: LogLogic Message Routing Errors	Displays all log forwarding errors on the LogLogic appliance to ensure all logs are archived properly.
205	HIPAA: McAfee AntiVirus: Attacks by Event ID	Displays McAfee AntiVirus attacks by Event ID.
206	HIPAA: McAfee AntiVirus: Attacks by Threat Name	Displays McAfee AntiVirus attacks by threat name.
207	HIPAA: McAfee AntiVirus: Attacks Detected	Displays attacks detected by McAfee AntiVirus.
208	HIPAA: Microsoft Operations Manager - Windows Accounts Activities	Displays all accounts activities on Windows servers to ensure authorized and appropriate access.
209	HIPAA: Microsoft Operations Manager - Windows Accounts Created	Displays all accounts created on Windows servers to ensure authorized and appropriate access.
210	HIPAA: Microsoft Operations Manager - Windows Accounts Enabled	Displays all accounts enabled on Windows servers to ensure authorized and appropriate access.

Serial Number	TIBCO LogLogic Report	Description
211	HIPAA: Microsoft Operations Manager - Windows Password Changes	Displays all password change activities on Windows servers to ensure authorized and appropriate access.
212	HIPAA: Microsoft Operations Manager - Windows Permissions Modified	Displays all permission modification activities on Windows servers to ensure authorized access.
213	HIPAA: Microsoft Operations Manager - Windows Policies Modified	Displays all policy modification activities on Windows servers to ensure authorized and appropriate access.
214	HIPAA: Microsoft Operations Manager - Windows Servers Restarted	Displays all Windows server restart activities to detect unusual activities.
215	HIPAA: Microsoft Sharepoint Content Deleted	Displays all events when content has been deleted from Microsoft Sharepoint.
216	HIPAA: Microsoft Sharepoint Content Updates	Displays all events when content is updated within Microsoft Sharepoint.
217	HIPAA: Microsoft Sharepoint Permissions Changed	Displays all user and group permission events to Microsoft Sharepoint.
218	HIPAA: Microsoft Sharepoint Policy Add, Remove, or Modify	Displays all events when a Microsoft Sharepoint policy is added, removed, or modified.
219	HIPAA: Microsoft SQL Server Configuration Changes	Displays Microsoft SQL database configuration changes.
220	HIPAA: Microsoft SQL Server Data Access	Displays data access events on Microsoft SQL Server databases.
221	HIPAA: Microsoft SQL Server Database Failed Logins	Displays failed Microsoft SQL Server database logins.
222	HIPAA: Microsoft SQL Server Database Successful Logins	Displays successful Microsoft SQL Server database logins.
223	HIPAA: Microsoft SQL Server Database Permission Events	Displays events related to Microsoft SQL Server database permission modifications.

Serial Number	TIBCO LogLogic Report	Description
224	HIPAA: Microsoft SQL Server Database User Additions and Deletions	Displays Microsoft SQL Server events related to creation and deletion of database users.
225	HIPAA: Microsoft SQL Server Password Changes	Displays password changes for Microsoft SQL Server database accounts.
226	HIPAA: Most Active Ports Through Firewall - Check Point	Displays the most active ports used through the Check Point firewall.
227	HIPAA: Most Active Ports Through Firewall - Cisco ASA	Displays the most active ports used through the Cisco ASA firewall.
228	HIPAA: Most Active Ports Through Firewall - Cisco FWSM	Displays the most active ports used through the Cisco FWSM firewall.
229	HIPAA: Most Active Ports Through Firewall - Cisco PIX	Displays the most active ports used through the Cisco PIX firewall.
230	HIPAA: Most Active Ports Through Firewall - Fortinet	Displays the most active ports used through the Fortinet firewall.
231	HIPAA: Most Active Ports Through Firewall - Juniper Firewall	Displays the most active ports used through the Juniper Firewall.
232	HIPAA: Most Active Ports Through Firewall - Nortel	Displays the most active ports used through the Nortel firewall.
233	HIPAA: NetApp Filer Audit Logs Cleared	Displays all audit logs clearing activities on NetApp Filer Audit to detect access violations or unusual activity.
234	HIPAA: NetApp Filer Audit Accounts Enabled	Displays all accounts enabled on NetApp Filer Audit to ensure authorized and appropriate access.
235	HIPAA: NetApp Filer Accounts Locked	Displays all accounts locked out of NetApp Filer to detect access violations or unusual activities.
236	HIPAA: NetApp Filer Audit Login Failed	Displays all NetApp Filer Audit login events which have failed.
237	HIPAA: NetApp Filer Audit Login Successful	Displays all NetApp Filer Audit login events which have succeeded.
238	HIPAA: NetApp Filer Audit Policies Modified	Displays all policy modification activities on NetApp Filer Audit to ensure authorized and appropriate access.

Serial Number	TIBCO LogLogic Report	Description
239	HIPAA: NetApp Filer File Activity	Displays all file activities on NetApp Filer.
240	HIPAA: NetApp Filer Login Failed	Displays all NetApp Filer login events which have failed.
241	HIPAA: NetApp Filer Login Successful	Displays all NetApp Filer login events which have succeeded.
242	HIPAA: NetApp Filer Password Changes	Displays all password change activities on NetApp Filer to ensure authorized and appropriate access.
243	HIPAA: NetApp Filer Snapshot Error	Displays events that indicate backup on the NetApp Filer has failed.
244	HIPAA: Oracle Database Failed Logins	Displays all failed login attempts to the Oracle database.
245	HIPAA: Oracle Database Configuration Changes	Displays Oracle database configuration changes.
246	HIPAA: Oracle Database Data Access	Displays data access events on Oracle databases.
247	HIPAA: Oracle Database Successful Logins	Displays successful Oracle database logins.
248	HIPAA: Oracle Database Permission Events	Displays events related to Oracle Server database role and privilege management.
249	HIPAA: Oracle Database User Additions and Deletions	Displays Oracle database events related to creation and deletion of database users.
250	HIPAA: PANOS: Attacks by Event ID	Displays Palo Alto Networks attacks by Event ID.
251	HIPAA: PANOS: Attacks by Threat Name	Displays Palo Alto Networks attacks by threat name.
252	HIPAA: PANOS: Attacks Detected	Displays attacks detected by Palo Alto Networks.
253	HIPAA: Password Changes on Windows Servers	Displays all password change activities on Windows servers to ensure authorized and appropriate access.
254	HIPAA: Periodic Review of Log Reports	Displays all review activities performed by administrators to ensure review for any access violations.

Serial Number	TIBCO LogLogic Report	Description
255	HIPAA: Periodic Review of User Access Logs	Displays all review activities performed by administrators to ensure review for any access violations.
256	HIPAA: Permissions Modified on Windows Servers	Displays all permission modification activities on Windows servers to ensure authorized access.
257	HIPAA: Policies Modified on Windows Servers	Displays all policy modification activities on Windows Servers to ensure authorized and appropriate access.
258	HIPAA: Pulse Connect Secure Policy Changed	Displays all configuration changes to the Pulse Connect Secure policies.
259	HIPAA: Pulse Connect Secure Successful Logins by IP	Displays all successful Pulse Connect Secure logins based on IP address.
260	HIPAA: Pulse Connect Secure Successful Logins by User	Displays all successful Pulse Connect Secure logins based on user.
261	HIPAA: Proxy Access to Applications	Displays all proxy-based access to applications to ensure appropriate and authorized access.
262	HIPAA: Proxy Access to Applications - Blue Coat Proxy	Displays all proxy-based access to applications to ensure appropriate and authorized access on Blue Coat Proxy.
263	HIIPAA: Proxy Access to Applications - Cisco WSA	Displays all proxy-based access to applications and authorized access on Cisco WSA.
264	HIPAA: Proxy Access to Applications - Microsoft IIS	Displays all proxy-based access to applications to ensure appropriate and authorized access on Microsoft IIS.
265	HIPAA: RACF Accounts Created	Displays all accounts created on RACF servers to ensure authorized and appropriate access.
266	HIPAA: RACF Accounts Deleted	Displays all accounts deleted on RACF servers to ensure authorized and appropriate access.
267	HIPAA: RACF Accounts Modified	Displays all events when a network user profile has been modified.
268	HIPAA: RACF Failed Logins	Displays all failed login attempts to review any access violations or unusual activity.
269	HIPAA: RACF Files Accessed	Displays all files accessed on RACF servers to ensure appropriate access.

Serial Number	TIBCO LogLogic Report	Description
270	HIPAA: RACF Password Changed	Displays all password change activities on RACF servers to ensure authorized and appropriate access.
271	HIPAA: RACF Permissions Changed	Displays all permission modification activities on RACF to ensure authorized access.
272	HIPAA: RACF Process Started	Displays all processes started on the RACF servers.
273	HIPAA: RACF Successful Logins	Displays successful logins to ensure only authorized personnel have access.
274	HIPAA: Sidewinder Configuration Changes	Displays Sidewinder configuration changes.
275	HIPAA: Software Update Successes on i5/OS	Displays all i5/OS successful events related to the system's software or patch update.
276	HIPAA: Successful Logins	Displays successful logins to ensure only authorized personnel have access.
277	HIPAA: Sybase ASE Database Configuration Changes	Displays configuration changes to the Sybase database.
278	HIPAA: Sybase ASE Database Data Access	Displays Sybase ASE events involving the SELECT statement.
279	HIPAA: Sybase ASE Database User Additions and Deletions	Displays Sybase database events related to creation and deletion of database users.
280	HIPAA: Sybase ASE Failed Logins	Displays failed Sybase ASE database logins.
281	HIPAA: Sybase ASE Successful Logins	Displays successful Sybase ASE database logins.
282	HIPAA: Symantec AntiVirus: Attacks by Threat Name	Displays Symantec AntiVirus attacks by threat name.
283	HIPAA: Symantec AntiVirus: Attacks Detected	Displays attacks detected by Symantec AntiVirus.
284	HIPAA: Symantec AntiVirus: Scans	Displays scans using Symantec AntiVirus.
285	HIPAA: Symantec AntiVirus: Updated	Displays updates to Symantec AntiVirus.

Serial Number	TIBCO LogLogic Report	Description
286	HIPAA: Symantec Endpoint Protection: Attacks by Threat Name	Displays Symantec Endpoint Protection attacks by threat name.
287	HIPAA: Symantec Endpoint Protection: Attacks Detected	Displays attacks detected by Symantec Endpoint Protection.
288	HIPAA: Symantec Endpoint Protection Configuration Changes	Displays Symantec Endpoint Protection configuration changes.
289	HIPAA: Symantec Endpoint Protection Password Changes	Displays all password change activities on Symantec Endpoint Protection to ensure authorized and appropriate access.
290	HIPAA: Symantec Endpoint Protection Policy Add, Remove, or Modify	Displays all events when a Symantec Endpoint Protection policy is added, removed, or modified.
291	HIPAA: Symantec Endpoint Protection: Scans	Displays scans using Symantec Endpoint Protection.
292	HIPAA: Symantec Endpoint Protection: Updated	Displays updates to Symantec Endpoint Protection.
293	HIPAA: System Restarted	Displays all logs related to system restarts.
294	HIPAA: TIBCO Administrator Password Changes	Displays all password change activities on TIBCO Administrator to ensure authorized and appropriate access.
295	HIPAA: TIBCO Administrator Permission Changes	Displays events related to TIBCO Administrator permission modifications.
296	HIPAA: TIBCO ActiveMatrix Administrator Permission Changes	Displays events related to TIBCO ActiveMatrix Administrator permission modifications.
297	HIPAA: TIBCO ActiveMatrix Administrator Failed Logins	Displays all TIBCO ActiveMatrix Administrator login events which have failed.
298	HIPAA: TIBCO ActiveMatrix Administrator Successful Logins	Displays successful logins to TIBCO ActiveMatrix Administrator to ensure only authorized personnel have access.
299	HIPAA: TrendMicro OfficeScan: Attacks Detected	Displays attacks detected by TrendMicro OfficeScan.

Serial Number	TIBCO LogLogic Report	Description
300	HIPAA: TrendMicro OfficeScan: Attacks Detected by Threat Name	Displays attacks detected by TrendMicro OfficeScan by threat name.
301	HIPAA: TrendMicro Control Manager: Attacks Detected	Displays attacks detected by TrendMicro Control Manager.
302	HIPAA: TrendMicro Control Manager: Attacks Detected by Threat Name	Displays attacks detected by TrendMicro Control Manager by threat name.
303	HIPAA: Unauthorized Login s	Displays all logins from unauthorized users to ensure appropriate access to data.
304	HIPAA: UNIX Failed Logins	Displays failed UNIX logins for known and unknown users.
305	HIPAA: vCenter Change Attributes	Displays information about modification of VMware vCenter and VMware ESX properties.
306	HIPAA: vCenter Data Move	Displays information about an entity that has been moved within the VMware vCenter infrastructure.
307	HIPAA: vCenter Datastore Events	Displays create, modify, and delete datastore events on VMware vCenter.
308	HIPAA: vCenter Failed Logins	Displays failed logins to the VMware vCenter console.
309	HIPAA: vCenter Modify Firewall Policy	Displays changes to the VMware ESX allowed services firewall policy.
310	HIPAA: vCenter Orchestrator Change Attributes	Displays information about modification of VMware vCenter Orchestrator properties.
311	HIPAA: vCenter Orchestrator Datastore Events	Displays create, modify, and delete datastore events on VMware vCenter Orchestrator.
312	HIPAA: vCenter Orchestrator Data Move	Displays information about an entity that has been moved within the VMware vCenter Orchestrator infrastructure.
313	HIPAA: vCenter Orchestrator Failed Logins	Displays all failed logins for VMware vCenter Orchestrator.
314	HIPAA: vCenter Orchestrator Virtual Machine Created	Displays information about a Virtual machine that has been created from VMware vCenter Orchestrator.

Serial Number	TIBCO LogLogic Report	Description
315	HIPAA: vCenter Orchestrator Virtual Machine Deleted	Displays information about a Virtual machine that has been deleted from VMware vCenter Orchestrator.
316	HIPAA: vCenter Orchestrator Virtual Machine Shutdown	Displays information about a Virtual machine that has been shutdown or paused from VMware vCenter Orchestrator console.
317	HIPAA: vCenter Orchestrator Virtual Machine Started	Displays information about a Virtual machine that has been started or resumed from VMware vCenter Orchestrator console.
318	HIPAA: vCenter Orchestrator vSwitch Added, Changed or Removed	Displays information about a vSwitch that has been added, modified or removed from VMware vCenter Orchestrator console.
319	HIPAA: vCenter Resource Usage Change	Displays information about resources that have changed on VMware vCenter.
320	HIPAA: vCenter Restart ESX Services	Displays information when VMware vCenter restarted services are running on VMware ESX Server.
321	HIPAA: vCenter Shutdown or Restart of ESX Server	Displays information when VMware ESX Server is shutdown or restarted from VMware vCenter console.
322	HIPAA: vCenter Successful Logins	Displays information about successful logins to the VMware vCenter console.
323	HIPAA: vCenter User Permission Change	Displays information about a permission role that has been added, changed, removed, or applied to a user on VMware vCenter server.
324	HIPAA: vCenter Virtual Machine Created	Displays information about a Virtual machine that has been created from a VMware vCenter console.
325	HIPAA: vCenter Virtual Machine Deleted	Displays information about a Virtual machine that has been deleted or removed from VMware vCenter console.
326	HIPAA: vCenter Virtual Machine Shutdown	Displays information about a Virtual machine that has been shutdown or paused from VMware vCenter console.
327	HIPAA: vCenter Virtual Machine Started	Displays information about a Virtual machine that has been started or resumed from VMware vCenter console.
328	HIPAA: vCenter vSwitch Added, Changed or Removed	Displays information about a vSwitch on VMware ESX server that has been added, modified, or removed from the VMware vCenter console.

Serial Number	TIBCO LogLogic Report	Description
329	HIPAA: vCloud Failed Logins	Displays failed logins to the VMware vCloud Director console.
330	HIPAA: vCloud Organization Created	Displays events created on Vmware vCloud Director organization.
331	HIPAA: vCloud Organization Deleted	Displays events deleted from VMware vCloud Director organization.
332	HIPAA: vCloud Organization Modified	Displays modified events of VMware vCloud Director organization.
333	HIPAA: vCloud Successful Logins	Displays successful logins to the VMware vCloud Director console.
334	HIPAA: vCloud User Created	Displays user-created events on VMware vCloud Director.
335	HIPAA: vCloud User Deleted or Removed	Displays users that have been deleted or removed from VMware vCloud Director.
336	HIPAA: vCloud vApp Created, Modified, or Deleted	Displays events created, modified, or deleted on VMware vCloud Director vApp.
337	HIPAA: vCloud vDC Created, Modified, or Deleted	Displays events created, modified, or deleted on the VMware vCloud Director virtual datacenter.
338	HIPAA: vShield Edge Configuration Changes	Displays changes to VMware vShield Edge policies.
339	HIPAA: VPN Sessions by Source IPs	Displays all VPN sessions categorized by source IP addresses.
340	HIPAA: VPN Users Accessing Corporate Network	Displays all users logging into the corporate network through Virtual Private Network to ensure appropriate access.
341	HIPAA: Web Access to Applications	Displays all web-based access to applications to ensure appropriate and authorized access.
342	HIPAA: Web Access to Applications - F5 BIG-IP TMOS	Displays all web-based access to applications to ensure appropriate and authorized access on F5 BIG-IP TMOS.
343	HIPAA: Web Access to Applications - Fortinet	Displays all web-based access to applications to ensure appropriate and authorized access on Fortinet.

Serial Number	TIBCO LogLogic Report	Description
344	HIPAA: Web Access to Applications - PANOS	Displays all web-based access to applications to ensure appropriate and authorized access on Palo Alto Networks.
345	HIPAA: Web Access to Appl ications - Microsoft IIS	Displays all web-based access to applications to ensure appropriate and authorized access on Microsoft IIS.
346	HIPAA: Windows Accounts Enabled	Displays all accounts enabled on Windows servers to ensure authorized and appropriate access.
347	HIPAA: Windows Accounts Locked	Displays all accounts locked out of Windows servers to detect access violations or unusual activities.
348	HIPAA: Windows Audit Logs Cleared	Displays all audit logs clearing activities on Windows servers to detect access violations or unusual activity.
349	HIPAA: Windows New Services Installed	Displays a list of new services installed on Windows Servers to ensure authorized access.
350	HIPAA: Windows Servers Restarted	Displays all Windows server restart activities to detect unusual activities.
351	HIPAA: Windows Software Update Activities	Displays all events related to the system's software or patch update.
352	HIPAA: Windows Software Update Failures	Displays all failed events related to the system's software or patch update.
353	HIPAA: Windows Software Update Successes	Displays all successful events related to the system's software or patch update.
354	HIPAA: Applications Under Attack - FireEye MPS	Displays all applications under attack as well as the attack signatures by FireEye MPS.
355	HIPAA: F5 BIG-IP TMOS Login Failed	Displays all F5 BIG-IP TMOS login events which have failed.
356	HIPAA: F5 BIG-IP TMOS Login Successful	Displays all F5 BIG-IP TMOS login events which have succeeded.
357	HIPAA: F5 BIG-IP TMOS Password Changes	Displays all password change activities on F5 BIG-IP TMOS to ensure authorized and appropriate access.
358	HIPAA: F5 BIG-IP TMOS Restarted	Displays all events when the F5 BIG-IP TMOS has been restarted.
359	HIPAA: FireEye MPS: Attacks by Event ID	Displays FireEye MPS attacks by Event ID.
360	HIPAA: FireEye MPS: Attacks Detected	Displays attacks detected by FireEye MPS.

Serial Number	TIBCO LogLogic Report	Description
361	HIPAA: FireEye MPS: Attacks by Threat Name	Displays FireEye MPS attacks by threat name.
362	HIPAA: Firewall Connections Accepted - F5 BIG-IP TMOS	Displays all traffic passing through the F5 BIG-IP TMOS device.
363	HIPAA: Firewall Connections Denied - F5 BIG-IP TMOS	Displays the applications that have been denied access the most by the F5 BIG-IP TMOS.
364	HIPAA: Files Accessed Through Pulse Connect Secure	Displays all files accessed through Pulse Connect Secure
365	HIPAA: Firewall Traffic Considered Risky - F5 BIG-IP TMOS	Displays F5 BIG-IP TMOS allowed firewall traffic that is considered risky.
366	HIPAA: Pulse Connect Secure Policy Change	Displays all configuration changes to the Pulse Connect Secure policies or configuration change.
367	HIPAA: Pulse Connect Secure Successful Logins by IP	Displays all successful Pulse Connect Secure logins based on IP address.
368	HIPAA: Pulse Connect Secure Successful Logins by User	Displays all successful Pulse Connect Secure logins based on user.
369	HIPAA: Web Access to Applications - F5 BIG-IP TMOS	Displays all web-based access to applications to ensure appropriate and authorized access on F5 BIG-IP TMOS.
370	HIPAA: F5 BIG-IP TMOS Risky Traffic	F5 BIG-IP TMOS traffic considered risky.
371	HIPAA: Anomalous IDS Alerts	Alert when IDS anomalies are above or below defined thresholds.

TIBCO LogLogic Alerts for HIPAA

The LogLogic® Compliance Suite - HIPAA Edition allows for the continuous monitoring of the IT infrastructure using behavioral-based alerts.

Serial Number	TIBCO LogLogic Alert	Description
1	HIPAA: Accounts Created	Alerts when a new account is created on servers.

Serial Number	TIBCO LogLogic Alert	Description
2	HIPAA: Accounts Deleted	Alerts when an account is deleted on servers.
3	HIPAA: Accounts Enabled	Alerts when an account has been enabled on servers.
4	HIPAA: Accounts Locked	Alerts when an account has been locked on servers.
5	HIPAA: Accounts Modified	Alerts when an account is modified on servers.
6	HIPAA: Active Directory Changes	Alerts when changes are made within Active Directory.
7	HIPAA: Anomalous Firewall Traffic	Alerts when firewall traffic patterns are out of the norm.
8	HIPAA: Anomalous IDS Alerts	Alerts when IDS anomalies are above or below defined thresholds.
9	HIPAA: Anomalous Total Log Traffic	Alerts when log traffic volume is out of the norm compared to the baseline.
10	HIPAA: Check Point Policy Changed	Alerts when a Check Point firewall's policy has been modified.
11	HIPAA: Cisco ISE, ACS Configuration Changed	Alerts when configuration changes are made to the Cisco ISE or Cisco SecureACS.
12	HIPAA: Cisco ISE, ACS Passwords Changed	Alerts when a user changes their password via Cisco ISE or Cisco SecureACS.
13	HIPAA: Cisco PIX, ASA, FWSM Commands Executed	Alerts when a Cisco PIX, ASA, or FWSM commands are executed.
14	HIPAA: Cisco PIX, ASA, FWSM Failover Disabled	Alerts when a Cisco PIX, ASA, or FWSM HA configuration is disabled.
15	HIPAA: Cisco PIX, ASA, FWSM Failover Performed	Alerts when a failover has occurred on the Cisco PIX, ASA, or FWSM devices.
16	HIPAA: Cisco PIX, ASA, FWSM Policy Changed	Alerts when a Cisco PIX, ASA, or FWSM firewall policy has been modified.
17	HIPAA: System Restarted	Alerts when system has been restarted.
18	HIPAA: Cisco PIX, ASA, FWSM Routing Failure	Alerts when routing failure occurred in the Cisco PIX, ASA, or FWSM devices.
19	HIPAA: Cisco Switch Policy Changed	Alerts when Cisco router or switch configuration has been modified.

Serial Number	TIBCO LogLogic Alert	Description
20	HIPAA: DB2 Database Configuration Change	Alerts when a configuration is changed on a DB2 database.
21	HIPAA: DB2 Database User Added or Dropped	Alerts when a user is added or dropped from a DB2 database.
22	HIPAA: DNS Server Shutdown	Alerts when DNS Server has been shutdown.
23	HIPAA: DNS Server Started	Alerts when DNS Server has been started.
24	HIPAA: Escalated Privileges	Alerts when a user or program has escalated the privileges.
25	HIPAA: F5 BIG-IP TMOS Risky Traffic	F5 BIG-IP TMOS traffic considered risky.
26	HIPAA: Firewall Traffic Considered Risky	Alerts on non HTTP, SSL, or SSH traffic passing through the firewall.
27	HIPAA: Group Members Added	Alerts when new members are added to user groups.
28	HIPAA: Group Members Deleted	Alerts when members are removed from user groups.
29	HIPAA: Groups Created	Alerts when new user groups are created.
30	HIPAA: Groups Deleted	Alerts when a user group is deleted.
31	HIPAA: Groups Modified	Alerts when a user group has been modified.
32	HIPAA: Guardium SQL Guard Config Changes	Alerts when a configuration is changed on Guardium SQL Database.
33	HIPAA: Guardium SQL Guard Data Access	Alerts when a select statement is made on Guardium SQL Database.
34	HIPAA: Guardium SQL Guard Logins	Alerts when a user logs into the Guardium SQL Database.
35	HIPAA: HP NonStop Audit Configuration Changed	Alerts when configuration changes are made to the HP NonStop Audit.
36	HIPAA: HP NonStop Audit Permission Changed	Alerts on HP NonStop Audit permission changed events.
37	HIPAA: i5/OS Network Profile Changes	Alerts when any changes are made to an i5/OS network profile.

Serial Number	TIBCO LogLogic Alert	Description
38	HIPAA: i5/OS Permission or Policy Change	Alerts when policies or permissions are changed on the i5/OS.
39	HIPAA: i5/OS Server or Service Status Change	Alerts when the i5/OS is restarted or a service stops or starts.
40	HIPAA: i5/OS Software Updates	Alerts when events related to the i5/OS software updates.
41	HIPAA: i5/OS User Profile Changes	Alerts when a user profile is changed on the i5/OS.
42	HIPAA: IBM AIX Password Changed	Alerts when an account password is changed on IBM AIX servers.
43	HIPAA: Juniper Firewall HA State Change	Alerts when Juniper Firewall has changed its failover state.
44	HIPAA: Juniper Firewall Peer Missing	Alerts when a Juniper Firewall HA peer is missing.
45	HIPAA: Juniper Firewall Policy Changes	Alerts when Juniper Firewall configuration is changed.
46	HIPAA: Juniper Firewall Policy Out of Sync	Alerts when the Juniper Firewall's policy is out of sync.
47	HIPAA: Juniper Firewall System Reset	Alerts when the Juniper Firewall has been reset to system default.
48	HIPAA: Juniper VPN Policy Change	Alerts when Juniper VPN policy or configuration change.
49	HIPAA: Logins Failed	Alerts when login failures are over the defined threshold.
50	HIPAA: Logins Succeeded	Alerts when successful logins are over the defined threshold.
51	HIPAA: LogLogic Disk Full	Alerts when the LogLogic appliance's disk is near full.
52	HIPAA: LogLogic DSM Configuration Changes	Alerts when a configuration is changed on LogLogic DSM database.
53	HIPAA: LogLogic DSM Data Access	Alerts when a select statement is made on LogLogic DSM database.
54	HIPAA: LogLogic DSM Logins	Alerts when a user logs into the LogLogic DSM database.
55	HIPAA: LogLogic File Retrieval Errors	Alerts when problems are detected during log file retrieval.

Serial Number	TIBCO LogLogic Alert	Description
56	HIPAA: LogLogic HA State Change	Alerts when the LogLogic appliance failover state changes.
57	HIPAA: LogLogic Management Center Passwords Changed	Alerts when users have changed their passwords.
58	HIPAA: LogLogic Management Center Upgrade Succeeded	Alerts for successful events related to the system's upgrade.
59	HIPAA: LogLogic Message Routing Errors	Alerts when problems are detected during message forwarding.
60	HIPAA: LogLogic Universal Collector Configuration Changed	Alerts when configuration changes are made to the LogLogic universal collector.
61	HIPAA: Microsoft Operations Manager - Permissions Changed	Alerts when user or group permissions have been changed.
62	HIPAA: Microsoft Operations Manager - Windows Passwords Changed	Alerts when users have changed their passwords.
63	HIPAA: Microsoft Operations Manager - Windows Policies Changed	Alerts when Windows policies changed.
64	HIPAA: Microsoft Sharepoint Content Deleted	Alerts on Microsoft Sharepoint content deleted events.
65	HIPAA: Microsoft Sharepoint Content Updated	Alerts on Microsoft Sharepoint content updated events.
66	HIPAA: Microsoft Sharepoint Permission Changed	Alerts on Microsoft Sharepoint permission changed events.
67	HIPAA: Microsoft Sharepoint Policies Added, Removed, Modified	Alerts on Microsoft Sharepoint policy additions, deletions, and modifications.
68	HIPAA: NetApp Authentication Failure	Alerts when NetApp authentication failure events occur.
69	HIPAA: NetApp Filer Audit Policies Changed	Alerts when NetApp Filer Audit policies changed.

Serial Number	TIBCO LogLogic Alert	Description
70	HIPAA: NetApp Filer Disk Failure	Alerts when a disk fails on a NetApp Filer.
71	HIPAA: NetApp Filer Disk Inserted	Alerts when a disk is inserted into the NetApp Filer.
72	HIPAA: NetApp Filer Disk Missing	Alerts when a disk is missing on the NetApp Filer device.
73	HIPAA: NetApp Filer Disk Pulled	Alerts when a RAID disk has been pulled from the Filer device.
74	HIPAA: NetApp Filer Disk Scrub Suspended	Alerts when the disk scrubbing process has been suspended.
75	HIPAA: NetApp Filer File System Full	Alerts when the file system is full on the NetApp Filer device.
76	HIPAA: NetApp Filer NIS Group Update	Alerts when the NIS group has been updated on the Filer device.
77	HIPAA: NetApp Filer Snapshot Error	Alerts when an error has been detected during a NetApp Filer snapshot.
78	HIPAA: NetApp Filer Unauthorized Mounting	Alerts when an unauthorized mount event occurs.
79	HIPAA: Oracle Database Configuration Change	Alerts when a ALTER or UPDATE command is executed on Oracle DB's.
80	HIPAA: Oracle Database Data Access	Alerts when Oracle tables are accessed.
81	HIPAA: Oracle Database Permissions Changed	Alerts when permissions are changed on Oracle databases.
82	HIPAA: Oracle Database User Added or Deleted	Alerts when a user is added or deleted from an Oracle database.
83	HIPAA: Pulse Connect Secure Policy Change	Alerts when Pulse Connect Secure policy or configuration change.
84	HIPAA: RACF Files Accessed	Alerts when files are accessed on the RACF servers.
85	HIPAA: RACF Passwords Changed	Alerts when users have changed their passwords.
86	HIPAA: RACF Permissions Changed	Alerts when user or group permissions have been changed.

Serial Number	TIBCO LogLogic Alert	Description
87	HIPAA: RACF Process Started	Alerts whenever a process is run on a RACF server.
88	HIPAA: Sidewinder Configuration Changed	Alerts when configuration changes are made to the Sidewinder.
89	HIPAA: Sybase ASE Database Config Changes	Alerts on Sybase ASE Database configuration change events.
90	HIPAA: Sybase ASE Database Data Access	Alerts on Sybase ASE Database data access events.
91	HIPAA: Symantec Endpoint Protection Configuration Changed	Alerts when configuration changes are made to the Symantec Endpoint Protection.
92	HIPAA: Symantec Endpoint Protection Policy Add, Delete, Modify	Alerts on Symantec Endpoint Protection additions, deletions, and modifications.
93	HIPAA: TIBCO ActiveMatrix Administrator Permission Changed	Alerts on TIBCO ActiveMatrix Administrator permission changed events.
94	HIPAA: System Restarted	Alerts when systems such as routers and switches have restarted.
95	HIPAA: vCenter Create Virtual Machine	Alerts when virtual machine has been created from VMware vCenter console.
96	HIPAA: vCenter Data Move	Alerts when entity has been moved within the VMware vCenter infrastructure.
97	HIPAA: vCenter Datastore Event	Alerts on create, modify, and delete datastore events on VMware vCenter.
98	HIPAA: vCenter Delete Virtual Machine	Alerts when a virtual machine has been deleted or removed from VMware vCenter console.
99	HIPAA: vCenter Firewall Policy Change	Alerts when changes to the VMware ESX allowed services firewall policy.
100	HIPAA: vCenter Orchestrator Create Virtual Machine	Alerts when the virtual machine has been created from VMware vCenter Orchestrator console.
101	HIPAA: vCenter Orchestrator Data Move	Alerts when an entity is moved within the VMware vCenter Orchestrator infrastructure.

Serial Number	TIBCO LogLogic Alert	Description
102	HIPAA: vCenter Orchestrator Datastore Events	Alerts on create, modify, and delete datastore events on VMware vCenter Orchestrator.
103	HIPAA: vCenter Orchestrator Delete Virtual Machine	Alerts when a virtual machine has been deleted or removed from VMware vCenter Orchestrator console.
104	HIPAA: vCenter Orchestrator Login Failed	Failed logins to the VMware vCenter Orchestrator console.
105	HIPAA: vCenter Orchestrator Virtual Machine Shutdown	Virtual machine has been shutdown or paused from VMware vCenter Orchestrator console.
106	HIPAA: vCenter Orchestrator Virtual Machine Started	Virtual machine has been started or resumed from VMware vCenter Orchestrator console.
107	HIPAA: vCenter Orchestrator vSwitch Add, Modify or Delete	vSwitch on VMware ESX server has been added, modified or removed from vCenter Orchestrator.
108	HIPAA: vCenter Permission Change	Alerts when a permission role has been added, changed, removed, or applied on VMware vCenter.
109	HIPAA: vCenter Restart ESX Services	Alerts when VMware vCenter restarted services running on VMware ESX Server.
110	HIPAA: vCenter Shutdown or Restart ESX	Alerts when VMware ESX Server is shutdown from vCenter console.
111	HIPAA: vCenter User Login Failed	Alerts on failed logins to the VMware vCenter console.
112	HIPAA: vCenter User Login Successful	Alerts on successful logins to the VMware vCenter console.
113	HIPAA: vCenter Virtual Machine Shutdown	Alerts when virtual machine has been shutdown or paused from VMware vCenter console.
114	HIPAA: vCenter Virtual Machine Started	Alerts when virtual machine has been started or resumed from VMware vCenter console.
115	HIPAA: vCenter vSwitch Add, Modify or Delete	Alerts when vSwitch on VMware ESX server has been added, modified or removed from vCenter.
116	HIPAA: vCloud Director Login Failed	Alerts on failed logins to the VMware vCloud Director console.

Serial Number	TIBCO LogLogic Alert	Description
117	HIPAA: vCloud Director Login Success	Alerts on successful logins to the VMware vCloud Director console.
118	HIPAA: vCloud Organization Created	Alerts when organization successfully created on VMware vCloud Director.
119	HIPAA: vCloud Organization Deleted	Alerts when organization successfully deleted on VMware vCloud Director.
120	HIPAA: vCloud Organization Modified	Alerts when organization successfully modified on VMware vCloud Director.
121	HIPAA: vCloud User Created	Alerts when a user successfully created on VMware vCloud Director.
122	HIPAA: vCloud User, Group, or Role Modified	Alerts when VMware vCloud Director user, group, or role has been modified.
123	HIPAA: vCloud vApp Created, Deleted, or Modified	Alerts when VMware vCloud Director vApp has been created, deleted, or modified.
124	HIPAA: vCloud vDC Created, Modified, or Deleted	Alerts when VMware vCloud Director Virtual Datacenters have been created, deleted, or modified.
125	HIPAA: vShield Edge Configuration Change	Alerts when configuration changes to VMware vShield Edge policies.
126	HIPAA: vShield Risky Traffic	Alerts when VMware vShield Edge traffic considered risky.
127	HIPAA: Windows Audit Log Cleared	Alerts when audit logs on Windows servers have been cleared.
128	HIPAA: Windows Files Accessed	Show files accessed on the Windows servers.
129	HIPAA: Windows Objects Create/Delete	Alerts when system level objects have been created or deleted.
130	HIPAA: Windows Passwords Changed	Alerts when users have changed their passwords.
131	HIPAA: Windows Permissions Changed	Alerts when user or group permissions have been changed.
132	HIPAA: Windows Policies Changed	Alerts when Windows policies changed.

Serial Number	TIBCO LogLogic Alert	Description
133	HIPAA: Windows Process Started	Alerts when a process has been started on a Windows server.
134	HIPAA: Windows Programs Accessed	Alerts when a program is accessed on a Windows server.
135	HIPAA: Windows Software Updates	Alerts when events related to the Windows' software updates.
136	HIPAA: Windows Software Updates Failed	Alerts when failed events related to the software updates.
137	HIPAA: Windows Software Updates Succeeded	Alerts for successful events related to the software updates.

TIBCO LogLogic Reports and Alerts Quick Reference

The following table provides a mapping between the reports and alerts provided by the Compliance Suite to the HIPAA compliance controls.

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.308(a)(3)(ii)(A)	Authorization and/or Supervision (Addressable)	**Compliance Suite Reports** HIPAA: Accepted VPN Connections - RADIUS HIPAA: Account Activities on UNIX Servers HIPAA: Account Activities on Windows Servers HIPAA: Accounts Created on NetApp Filer HIPAA: Accounts Created on NetApp Filer Audit HIPAA: Accounts Created on Sidewinder HIPAA: Accounts Created on Symantec Endpoint Protection HIPAA: Accounts Created on TIBCO Administrator HIPAA: Accounts Created on UNIX Servers HIPAA: Accounts Created on Windows Servers HIPAA: Accounts Deleted on NetApp Filer HIPAA: Accounts Deleted on NetApp Filer Audit HIPAA: Accounts Deleted on Sidewinder HIPAA: Accounts Deleted on Symantec Endpoint Protection HIPAA: Accounts Deleted on TIBCO Administrator HIPAA: Accounts Deleted on TIBCO ActiveMatrix Administrator HIPAA: Accounts Deleted on UNIX Servers HIPAA: Accounts Deleted on Windows Servers HIPAA: Administrators Activities on Servers HIPAA: Check Point Management Station Login HIPAA: Cisco ISE, ACS Accounts Created HIPAA: Cisco ISE, ACS Accounts Removed HIPAA: DB2 Database Failed Logins HIPAA: DB2 Database Successful Logins HIPAA: DHCP Granted/Renewed Activities on Microsoft DHCP HIPAA: DHCP Granted/Renewed Activities on VMware vShield

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.308(a)(3)(ii)(A)	Authorization and/or Supervision (Addressable)	**Compliance Suite Reports** (Cont.) HIPAA: Escalated Privilege Activities on Servers HIPAA: ESX Accounts Activities HIPAA: ESX Accounts Created HIPAA: ESX Accounts Deleted HIPAA: ESX Failed Logins HIPAA: ESX Group Activities HIPAA: ESX Logins Failed Unknown User HIPAA: ESX Logins Succeeded HIPAA: F5 BIG-IP TMOS Login Failed HIPAA: F5 BIG-IP TMOS Login Successful HIPAA: Failed Logins HIPAA: Files Accessed on NetApp Filer Audit HIPAA: Files Accessed on Servers HIPAA: Files Accessed through Juniper SSL VPN (Secure Access) HIPAA: Files Accessed through PANOS HIPAA: Group Activities on NetApp Filer Audit HIPAA: Group Activities on Symantec Endpoint Protection HIPAA: Group Activities on TIBCO ActiveMatrix Administrator HIPAA: Group Activities on UNIX Servers HIPAA: Group Activities on Windows Servers HIPAA: Guardium SQL Guard Audit Logins HIPAA: Guardium SQL Guard Logins HIPAA: HP NonStop Audit Login Failed HIPAA: HP NonStop Audit Login Successful HIPAA: i5/OS Files Accessed HIPAA: i5/OS Network User Login Failed HIPAA: i5/OS Network User Login Successful HIPAA: i5/OS Network User Profile Creation HIPAA: i5/OS Network User Profile Deletion HIPAA: i5/OS User Login Failed HIPAA: i5/OS User Login Successful HIPAA: i5/OS User Profile Creation

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		HIPAA: Juniper SSL VPN Successful Logins by IP

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.308(a)(3)(ii)(A)	Authorization and/or Supervision (Addressable)	**Compliance Suite Reports** (Cont.) HIPAA: Juniper SSL VPN Successful Logins by User HIPAA: Juniper SSL VPN (Secure Access) Successful Logins by IP HIPAA: Juniper SSL VPN (Secure Access) Successful Logins by User HIPAA: Logins by Authentication Type HIPAA: LogLogic DSM Logins HIPAA: LogLogic Management Center Account Activities HIPAA: LogLogic Management Center Login HIPAA: Microsoft Operations Manager - Windows Accounts Activities HIPAA: Microsoft Operations Manager - Windows Accounts Created HIPAA: Microsoft Operations Manager - Windows Accounts Enabled HIPAA: Microsoft Sharepoint Content Deleted HIPAA: Microsoft Sharepoint Content Updates HIPAA: Microsoft SQL Server Database Failed Logins HIPAA: Microsoft SQL Server Database Successful Logins HIPAA: NetApp Filer Accounts Locked HIPAA: NetApp Filer Audit Accounts Enabled HIPAA: NetApp Filer Audit Login Failed HIPAA: NetApp Filer Audit Login Successful HIPAA: NetApp Filer File Activity HIPAA: NetApp Filer Login Failed HIPAA: NetApp Filer Login Successful HIPAA: Oracle Database Failed Logins HIPAA: Oracle Database Successful Logins HIPAA: RACF Accounts Created HIPAA: RACF Accounts Deleted HIPAA: RACF Failed Logins HIPAA: RACF Files Accessed HIPAA: RACF Successful Logins HIPAA: Successful Logins

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		HIPAA: Sybase ASE Failed Logins

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.308(a)(3)(ii)(A)	Authorization and/or Supervision (Addressable)	**Compliance Suite Reports** (Cont.) HIPAA: Sybase ASE Successful Logins HIPAA: TIBCO ActiveMatrix Administrator Failed Logins HIPAA: TIBCO ActiveMatrix Administrator Successful Logins HIPAA: Unauthorized Logins HIPAA: UNIX Failed Logins HIPAA: vCenter Datastore Events HIPAA: vCenter Data Move HIPAA: vCenter Failed Logins HIPAA: vCenter Orchestrator Datastore Events HIPAA: vCenter Orchestrator Data Move HIPAA: vCenter Orchestrator Failed Logins HIPAA: vCenter Successful Logins HIPAA: vCloud Failed Logins HIPAA: vCloud Successful Logins HIPAA: vCloud User Created HIPAA: vCloud User Deleted or Removed HIPAA: VPN Users Accessing Corporate Network HIPAA: Windows Accounts Enabled HIPAA: Windows Accounts Locked Compliance Suite Alerts HIPAA: Accounts Created HIPAA: Accounts Deleted HIPAA: Accounts Enabled HIPAA: Accounts Locked HIPAA: Escalated Privileges HIPAA: Groups Created HIPAA: Groups Deleted HIPAA: Groups Modified HIPAA: Guardium SQL Guard Logins HIPAA: Logins Failed HIPAA: Logins Succeeded HIPAA: LogLogic DSM Logins HIPAA: Microsoft Sharepoint Content Deleted

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		HIPAA: Microsoft Sharepoint Content Updated
164.308(a)(3)(ii)(A)	Authorization and/or Supervision (Addressable)	Compliance Suite Alerts (Cont.) HIPAA: NetApp Authentication Failure HIPAA: NetApp Filer NIS Group Update HIPAA: NetApp Filer Unauthorized Mounting HIPAA: RACF Files Accessed HIPAA: vCenter Datastore Event HIPAA: vCenter Data Move HIPAA: vCenter Orchestrator Data Move HIPAA: vCenter Orchestrator Datastore Events HIPAA: vCenter Orchestrator Login Failed HIPAA: vCenter User Login Failed HIPAA: vCenter User Login Successful HIPAA: vCloud Director Login Failed HIPAA: vCloud Director Login Success HIPAA: vCloud User Created HIPAA: Windows Files Accessed HIPAA: Windows Programs Accessed

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.308(a)(3)(ii)(C)	Termination Procedures (Addressable)	**Compliance Suite Reports** HIPAA: Accepted VPN Connections - RADIUS HIPAA: Account Activities on UNIX Servers HIPAA: Account Activities on Windows Servers HIPAA: Accounts Changed on NetApp Filer HIPAA: Accounts Changed on TIBCO Administrator HIPAA: Accounts Changed on TIBCO ActiveMatrix Administrator HIPAA: Accounts Changed on UNIX Servers HIPAA: Accounts Changed on Windows Servers HIPAA: Accounts Deleted on NetApp Filer HIPAA: Accounts Deleted on NetApp Filer Audit HIPAA: Accounts Deleted on Sidewinder HIPAA: Accounts Deleted on Symantec Endpoint Protection HIPAA: Accounts Deleted on TIBCO Administrator HIPAA: Accounts Deleted on TIBCO ActiveMatrix Administrator HIPAA: Accounts Deleted on UNIX Servers HIPAA: Accounts Deleted on Windows Servers HIPAA: Check Point Management Station Login HIPAA: Cisco ISE, ACS Accounts Removed HIPAA: Creation and Deletion of System Level Objects: DB2 Database HIPAA: Creation and Deletion of System Level Objects: Oracle HIPAA: Creation and Deletion of System Level Objects: SQL Server HIPAA: Creation and Deletion of System Level Objects: Windows HIPAA: DB2 Database Configuration Changes HIPAA: DB2 Database Failed Logins HIPAA: DB2 Database Successful Logins HIPAA: DB2 Database User Additions and Deletions HIPAA: ESX Accounts Activities HIPAA: ESX Accounts Deleted

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		HIPAA: ESX Failed Logins HIPAA: ESX Group Activities

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.308(a)(3)(ii)(C)	Termination Procedures (Addressable)	**Compliance Suite Reports** (Cont.) HIPAA: ESX Logins Failed Unknown User HIPAA: ESX Logins Succeeded HIPAA: F5 BIG-IP TMOS Login Failed HIPAA: F5 BIG-IP TMOS Login Successful HIPAA: Failed Logins HIPAA: Group Activities on NetApp Filer Audit HIPAA: Group Activities on Symantec Endpoint Protection HIPAA: Group Activities on TIBCO ActiveMatrix Administrator HIPAA: Group Activities on UNIX Servers HIPAA: Group Activities on Windows Servers HIPAA: Guardium SQL Guard Audit Configuration Changes HIPAA: Guardium SQL Guard Audit Data Access HIPAA: Guardium SQL Guard Audit Logins HIPAA: Guardium SQL Guard Configuration Changes HIPAA: Guardium SQL Guard Data Access HIPAA: Guardium SQL Guard Logins HIPAA: HP NonStop Audit Configuration Changes HIPAA: HP NonStop Audit Login Failed HIPAA: HP NonStop Audit Login Successful HIPAA: HP NonStop Audit Object Changes HIPAA: HP NonStop Audit Permissions Changed HIPAA: i5/OS Network User Login Failed HIPAA: i5/OS Network User Login Successful HIPAA: i5/OS Network User Profile Deletion HIPAA: i5/OS Network User Profile Modified HIPAA: i5/OS Object Permissions Modified HIPAA: i5/OS User Login Failed HIPAA: i5/OS User Login Successful HIPAA: i5/OS User Profile Modifications HIPAA: Juniper SSL VPN Successful Logins by IP HIPAA: Juniper SSL VPN Successful Logins by User

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		HIPAA: Juniper SSL VPN (Secure Access) Successful Logins by IP

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.308(a)(3)(ii)(C)	Termination Procedures (Addressable)	**Compliance Suite Reports** (Cont.) HIPAA: Juniper SSL VPN (Secure Access) Successful Logins by User HIPAA: LogLogic DSM Configuration Changes HIPAA: LogLogic DSM Data Access HIPAA: LogLogic DSM Logins HIPAA: LogLogic Management Center Account Activities HIPAA: LogLogic Management Center Login HIPAA: LogLogic Universal Collector Configuration Changes HIPAA: Microsoft Operations Manager - Windows Accounts Activities HIPAA: Microsoft Operations Manager - Windows Permissions Modified HIPAA: Microsoft Sharepoint Content Deleted HIPAA: Microsoft Sharepoint Content Updates HIPAA: Microsoft Sharepoint Permissions Changed HIPAA: Microsoft SQL Server Configuration Changes HIPAA: Microsoft SQL Server Data Access HIPAA: Microsoft SQL Server Database Failed Logins HIPAA: Microsoft SQL Server Database Successful Logins HIPAA: Microsoft SQL Server Database Permission Events HIPAA: Microsoft SQL Server Database User Additions and Deletions HIPAA: Microsoft SQL Server Password Changes HIPAA: NetApp Filer Audit Login Failed HIPAA: NetApp Filer Audit Login Successful HIPAA: NetApp Filer Login Failed HIPAA: NetApp Filer Login Successful HIPAA: Oracle Database Configuration Changes HIPAA: Oracle Database Data Access HIPAA: Oracle Database Failed Logins HIPAA: Oracle Database Successful Logins

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		HIPAA: Oracle Database Permission Events

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.308(a)(3)(ii)(C)	Termination Procedures (Addressable)	**Compliance Suite Reports** (Cont.) HIPAA: Oracle Database User Additions and Deletions HIPAA: Permissions Modified on Windows Servers HIPAA: RACF Accounts Deleted HIPAA: RACF Accounts Modified HIPAA: RACF Failed Logins HIPAA: RACF Permissions Changed HIPAA: RACF Successful Logins HIPAA: Successful Logins HIPAA: Sybase ASE Database Configuration Changes HIPAA: Sybase ASE Database Data Access HIPAA: Sybase ASE Database User Additions and Deletions HIPAA: Sybase ASE Failed Logins HIPAA: Sybase ASE Successful Logins HIPAA: TIBCO Administrator Permission Changes HIPAA: TIBCO ActiveMatrix Administrator Failed Logins HIPAA: TIBCO ActiveMatrix Administrator Permission Changes HIPAA: TIBCO ActiveMatrix Administrator Successful Logins HIPAA: UNIX Failed Logins HIPAA: vCenter Failed Logins HIPAA: vCenter Orchestrator Failed Logins HIPAA: vCenter Successful Logins HIPAA: vCenter User Permission Change HIPAA: vCloud Failed Logins HIPAA: vCloud Successful Logins HIPAA: vCloud User Deleted or Removed HIPAA: VPN Users Accessing Corporate Network Compliance Suite Alerts HIPAA: Accounts Deleted HIPAA: Accounts Modified HIPAA: DB2 Database Configuration Change

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		HIPAA: DB2 Database User Added or Dropped

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.308(a)(3)(ii)(C)	Termination Procedures (Addressable)	**Compliance Suite Alerts** (Cont.) HIPAA: Group Members Deleted HIPAA: Groups Deleted HIPAA: Groups Modified HIPAA: Guardium SQL Guard Config Changes HIPAA: Guardium SQL Guard Data Access HIPAA: Guardium SQL Guard Logins HIPAA: HP NonStop Audit Configuration Changed HIPAA: HP NonStop Audit Permission Changed HIPAA: i5/OS Network Profile Changes HIPAA: i5/OS Permission or Policy Change HIPAA: i5/OS User Profile Changes HIPAA: Logins Failed HIPAA: Logins Succeeded HIPAA: LogLogic DSM Configuration Changes HIPAA: LogLogic DSM Data Access HIPAA: LogLogic DSM Logins HIPAA: LogLogic Universal Collector Configuration Changed HIPAA: Microsoft Operations Manager - Permissions Changed HIPAA: Microsoft Sharepoint Content Deleted HIPAA: Microsoft Sharepoint Content Updated HIPAA: Microsoft Sharepoint Permission Changed HIPAA: Oracle Database Configuration Change HIPAA: Oracle Database Data Access HIPAA: Oracle Database Permissions Changed HIPAA: Oracle Database User Added or Deleted HIPAA: RACF Permissions Changed HIPAA: Sybase ASE Database Config Changes HIPAA: Sybase ASE Database Data Access HIPAA: TIBCO ActiveMatrix Administrator Permission Changed HIPAA: vCenter Orchestrator Login Failed HIPAA: vCenter Permission Change HIPAA: vCenter User Login Failed

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.308(a)(4)(ii)(A)	Isolating Health Care Clearinghouse Functions (Required)	**Compliance Suite Reports** HIPAA: vCenter User Login Successful HIPAA: vCloud Director Login Failed HIPAA: vCloud Director Login Success HIPAA: vCloud User, Group, or Role Modified HIPAA: Windows Permissions Changed HIPAA: Check Point Object Activity HIPAA: Check Point Configuration Changes HIPAA: Cisco ISE, ACS Configuration Changes HIPAA: Cisco PIX, ASA, FWSM Policy Changed HIPAA: Cisco Switch Policy Changes HIPAA: Firewall Connections Accepted - Check Point HIPAA: Firewall Connections Accepted - Cisco ASA HIPAA: Firewall Connections Accepted - Cisco FWSM HIPAA: Firewall Connections Accepted - Cisco IOS HIPAA: Firewall Connections Accepted - Cisco Netflow HIPAA: Firewall Connections Accepted - Cisco NXOS HIPAA: Firewall Connections Accepted - Cisco PIX HIPAA: Firewall Connections Accepted - F5 BIG-IP TMOS HIPAA: Firewall Connections Accepted - Fortinet HIPAA: Firewall Connections Accepted - Juniper Firewall HIPAA: Firewall Connections Accepted - Juniper JunOS HIPAA: Firewall Connections Accepted - Juniper RT Flow HIPAA: Firewall Connections Accepted - Nortel HIPAA: Firewall Connections Accepted - PANOS HIPAA: Firewall Connections Accepted - Sidewinder HIPAA: Firewall Connections Accepted - VMware vShield HIPAA: Firewall Connections Denied - Check Point HIPAA: Firewall Connections Denied - Cisco ASA

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		HIPAA: Firewall Connections Denied - Cisco FWSM HIPAA: Firewall Connections Denied - Cisco IOS HIPAA: Pulse Connect Secure Policy Change

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.308(a)(4)(ii)(A)	Isolating Health Care Clearinghouse Functions (Required)	**Compliance Suite Reports** (Cont.) HIPAA: Firewall Connections Denied - Cisco NXOS HIPAA: Firewall Connections Denied - Cisco PIX HIPAA: Firewall Connections Denied - Cisco Router HIPAA: Firewall Connections Denied - F5 BIG-IP TMOS HIPAA: Firewall Connections Denied - Fortinet HIPAA: Firewall Connections Denied - Juniper Firewall HIPAA: Firewall Connections Denied - Juniper JunOS HIPAA: Firewall Connections Denied - Juniper RT Flow HIPAA: Firewall Connections Denied - Nortel HIPAA: Firewall Connections Denied - PANOS HIPAA: Firewall Connections Denied - Sidewinder HIPAA: Firewall Connections Denied - VMware vShield HIPAA: Firewall Traffic Considered Risky - Cisco PIX HIPAA: Firewall Traffic Considered Risky - Check Point HIPAA: Firewall Traffic Considered Risky - Cisco ASA HIPAA: Firewall Traffic Considered Risky - Cisco FWSM HIPAA: Firewall Traffic Considered Risky - Cisco IOS HIPAA: Firewall Traffic Considered Risky - Cisco Netflow HIPAA: Firewall Traffic Considered Risky - F5 BIG-IP TMOS HIPAA: Firewall Traffic Considered Risky - Fortinet HIPAA: Firewall Traffic Considered Risky - Juniper Firewall HIPAA: Firewall Traffic Considered Risky - Juniper JunOS HIPAA: Firewall Traffic Considered Risky - Juniper RT Flow HIPAA: Firewall Traffic Considered Risky - Nortel

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		HIPAA: Firewall Traffic Considered Risky - PANOS HIPAA: Firewall Traffic Considered Risky - Sidewinder HIPAA: Firewall Traffic Considered Risky - VMware vShield HIPAA: Juniper Firewall Policy Changed

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.308(a)(4)(ii)(A)	Isolating Health Care Clearinghouse Functions (Required)	**Compliance Suite Reports** (Cont.) HIPAA: Juniper SSL VPN (Secure Access) Policy Changed HIPAA: Most Active Ports Through Firewall - Check Point HIPAA: Most Active Ports Through Firewall - Cisco ASA HIPAA: Most Active Ports Through Firewall - Cisco FWSM HIPAA: Most Active Ports Through Firewall - Cisco PIX HIPAA: Most Active Ports Through Firewall - Fortinet HIPAA: Most Active Ports Through Firewall - Juniper Firewall HIPAA: Most Active Ports Through Firewall - Nortel HIPAA: NetApp Filer Audit Policies Modified HIPAA: Sidewinder Configuration Changes HIPAA: Symantec Endpoint Protection Configuration Changes HIPAA: Symantec Endpoint Protection Policy Add, Remove, or Modify HIPAA: vCenter Change Attributes HIPAA: vCenter Modify Firewall Policy HIPAA: vCenter Orchestrator Change Attributes HIPAA: vCenter Orchestrator Virtual Machine Created HIPAA: vCenter Orchestrator Virtual Machine Deleted HIPAA: vCenter Orchestrator vSwitch Added, Changed or Removed HIPAA: vCenter Resource Usage Change HIPAA: vCenter Virtual Machine Created HIPAA: vCenter Virtual Machine Deleted HIPAA: vCenter vSwitch Added, Changed or Removed HIPAA: vCloud Organization Created HIPAA: vCloud Organization Deleted HIPAA: vCloud Organization Modified

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		HIPAA: vCloud vApp Created, Modified, or Deleted HIPAA: vCloud vDC Created, Modified, or Deleted HIPAA: vShield Edge Configuration Changes
164.308(a)(4)(ii)(A)	Isolating Health Care Clearinghouse Functions (Required)	**Compliance Suite Alerts** HIPAA: Anomalous Firewall Traffic HIPAA: Anomalous Total Log Traffic HIPAA: Check Point Policy Changed HIPAA: Cisco ISE, ACS Configuration Changed HIPAA: Cisco PIX, ASA, FWSM Policy Changed HIPAA: Cisco Switch Policy Changed HIPAA: F5 BIG-IP TMOS Risky Traffic HIPAA: Firewall Traffic Considered Risky HIPAA: Juniper Firewall Policy Changes HIPAA: Juniper VPN Policy Change HIPAA: Sidewinder Configuration Changed HIPAA: Symantec Endpoint Protection Configuration Changed HIPAA: vCenter Create Virtual Machine HIPAA: vCenter Delete Virtual Machine HIPAA: vCenter Firewall Policy Change HIPAA: vCenter Orchestrator Create Virtual Machine HIPAA: vCenter Orchestrator Delete Virtual Machine HIPAA: vCenter Orchestrator vSwitch Add, Modify or Delete HIPAA: vCenter vSwitch Add, Modify or Delete HIPAA: vCloud Organization Created HIPAA: vCloud Organization Deleted HIPAA: vCloud Organization Modified HIPAA: vCloud vApp Created, Deleted, or Modified HIPAA: vCloud vDC Created, Modified, or Deleted HIPAA: vShield Edge Configuration Change HIPAA: vShield Risky Traffic

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.308(a)(4)(ii)(B)	Access Authorization (Addressable)	**Compliance Suite Reports** HIPAA: Accepted VPN Connections - RADIUS HIPAA: Account Activities on UNIX Servers HIPAA: Account Activities on Windows Servers HIPAA: Accounts Created on NetApp Filer HIPAA: Accounts Created on NetApp Filer Audit HIPAA: Accounts Created on Sidewinder HIPAA: Accounts Created on Symantec Endpoint Protection HIPAA: Accounts Created on TIBCO ActiveMatrix Administrator HIPAA: Accounts Created on TIBCO Administrator HIPAA: Accounts Created on UNIX Servers HIPAA: Accounts Created on Windows Servers HIPAA: Accounts Deleted on NetApp Filer HIPAA: Accounts Deleted on NetApp Filer Audit HIPAA: Accounts Deleted on Sidewinder HIPAA: Accounts Deleted on Symantec Endpoint Protection HIPAA: Accounts Deleted on TIBCO Administrator HIPAA: Accounts Deleted on TIBCO ActiveMatrix Administrator HIPAA: Accounts Deleted on UNIX Servers HIPAA: Accounts Deleted on Windows Servers HIPAA: Check Point Management Station Login HIPAA: Cisco ISE, ACS Accounts Created HIPAA: Cisco ISE, ACS Accounts Removed HIPAA: Cisco ISE, ACS Password Changes HIPAA: Creation and Deletion of System Level Objects: DB2 Database HIPAA: Creation and Deletion of System Level Objects: Oracle HIPAA: Creation and Deletion of System Level Objects: SQL Server HIPAA: Creation and Deletion of System Level Objects: Windows HIPAA: DB2 Database Configuration Changes

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.308(a)(4)(ii)(B)	Access Authorization (Addressable)	**Compliance Suite Reports** (Cont.) HIPAA: DB2 Database Failed Logins HIPAA: DB2 Database Successful Logins HIPAA: DB2 Database User Additions and Deletions HIPAA: Denied VPN Connections - RADIUS HIPAA: DHCP Granted/Renewed Activities on Microsoft DHCP HIPAA: DHCP Granted/Renewed Activities on VMware vShield HIPAA: ESX Accounts Activities HIPAA: ESX Accounts Created HIPAA: ESX Accounts Deleted HIPAA: ESX Failed Logins HIPAA: ESX Group Activities HIPAA: ESX Kernel log daemon terminating HIPAA: ESX Kernel logging Stop HIPAA: ESX Logins Failed Unknown User HIPAA: ESX Logins Succeeded HIPAA: ESX Syslogd Restart HIPAA: F5 BIG-IP TMOS Login Failed HIPAA: F5 BIG-IP TMOS Login Successful HIPAA: F5 BIG-IP TMOS Password Changes HIPAA: Failed Logins HIPAA: Group Activities on UNIX Servers HIPAA: Group Activities on Windows Servers HIPAA: Guardium SQL Guard Audit Configuration Changes HIPAA: Guardium SQL Guard Audit Data Access HIPAA: Guardium SQL Guard Audit Logins HIPAA: Guardium SQL Guard Configuration Changes HIPAA: Guardium SQL Guard Data Access HIPAA: Guardium SQL Guard Logins HIPAA: Group Activities on NetApp Filer Audit HIPAA: Group Activities on Symantec Endpoint Protection

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		HIPAA: Group Activities on TIBCO ActiveMatrix Administrator
164.308(a)(4)(ii)(B)	Access Authorization (Addressable)	**Compliance Suite Reports** (Cont.) HIPAA: HP NonStop Audit Configuration Changes HIPAA: HP NonStop Audit Login Failed HIPAA: HP NonStop Audit Login Successful HIPAA: HP NonStop Audit Permissions Changed HIPAA: i5/OS DST Password Reset HIPAA: i5/OS Network User Login Failed HIPAA: i5/OS Network User Login Successful HIPAA: i5/OS Network User Profile Creation HIPAA: i5/OS Network User Profile Deletion HIPAA: i5/OS Object Permissions Modified HIPAA: i5/OS Service Started HIPAA: i5/OS User Login Failed HIPAA: i5/OS User Login Successful HIPAA: i5/OS User Profile Creation HIPAA: Juniper SSL VPN Successful Logins by IP HIPAA: Juniper SSL VPN Successful Logins by User HIPAA: Juniper SSL VPN (Secure Access) Successful Logins by IP HIPAA: Juniper SSL VPN (Secure Access) Successful Logins by User HIPAA: LogLogic DSM Configuration Changes HIPAA: LogLogic DSM Data Access HIPAA: LogLogic DSM Logins HIPAA: LogLogic Management Center Account Activities HIPAA: LogLogic Management Center Login HIPAA: LogLogic Management Center Password Changes HIPAA: LogLogic Universal Collector Configuration Changes HIPAA: Microsoft Operations Manager - Windows Accounts Activities HIPAA: Microsoft Operations Manager - Windows Accounts Created

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.308(a)(4)(ii)(B)	Access Authorization (Addressable)	**Compliance Suite Reports** (Cont.) HIPAA: Microsoft Operations Manager - Windows Password Changes HIPAA: Microsoft Operations Manager - Windows Permissions Modified HIPAA: Microsoft Operations Manager - Windows Policies Modified HIPAA: Microsoft Sharepoint Content Deleted HIPAA: Microsoft Sharepoint Content Updates HIPAA: Microsoft Sharepoint Permissions Changed HIPAA: Microsoft Sharepoint Policy Add, Remove, or Modify HIPAA: Microsoft SQL Server Configuration Changes HIPAA: Microsoft SQL Server Data Access HIPAA: Microsoft SQL Server Database Failed Logins HIPAA: Microsoft SQL Server Database Successful Logins HIPAA: Microsoft SQL Server Database Permission Events HIPAA: Microsoft SQL Server Database User Additions and Deletions HIPAA: Microsoft SQL Server Password Changes HIPAA: Most Active Ports Through Firewall - Check Point HIPAA: Most Active Ports Through Firewall - Cisco ASA HIPAA: Most Active Ports Through Firewall - Cisco FWSM HIPAA: Most Active Ports Through Firewall - Cisco PIX HIPAA: Most Active Ports Through Firewall - Fortinet HIPAA: Most Active Ports Through Firewall - Juniper Firewall HIPAA: Most Active Ports Through Firewall - Nortel HIPAA: NetApp Filer Audit Login Failed HIPAA: NetApp Filer Audit Login Successful HIPAA: NetApp Filer Login Failed

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		HIPAA: NetApp Filer Login Successful HIPAA: NetApp Filer Password Changes

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.308(a)(4)(ii)(B)	Access Authorization (Addressable)	**Compliance Suite Reports** (Cont.) HIPAA: Oracle Database Configuration Changes HIPAA: Oracle Database Data Access HIPAA: Oracle Database Failed Logins HIPAA: Oracle Database Successful Logins HIPAA: Oracle Database Permission Events HIPAA: Oracle Database User Additions and Deletions HIPAA: Password Changes on Windows Servers HIPAA: Permissions Modified on Windows Servers HIPAA: Policies Modified on Windows Servers HIPAA: Proxy Access to Applications HIPAA: Proxy Access to Applications - Blue Coat Proxy HIPAA: Proxy Access to Applications - Microsoft IIS HIPAA: Proxy Access to Applications - Cisco WSA HIPAA: RACF Accounts Created HIPAA: RACF Accounts Deleted HIPAA: RACF Failed Logins HIPAA: RACF Password Changed HIPAA: RACF Permissions Changed HIPAA: RACF Process Started HIPAA: RACF Successful Logins HIPAA: Successful Logins HIPAA: Sybase ASE Database Configuration Changes HIPAA: Sybase ASE Database Data Access HIPAA: Sybase ASE Database User Additions and Deletions HIPAA: Sybase ASE Failed Logins HIPAA: Sybase ASE Successful Logins HIPAA: Symantec Endpoint Protection Password Changes HIPAA: TIBCO ActiveMatrix Administrator Failed Logins HIPAA: TIBCO ActiveMatrix Administrator Permission Changes

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		HIPAA: TIBCO ActiveMatrix Administrator Successful Logins

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.308(a)(4)(ii)(B)	Access Authorization (Addressable)	**Compliance Suite Reports** (Cont.) HIPAA: TIBCO Administrator Password Changes HIPAA: TIBCO Administrator Permission Changes HIPAA: UNIX Failed Logins HIPAA: vCenter User Permission Change HIPAA: vCenter Datastore Events HIPAA: vCenter Data Move HIPAA: vCenter Failed Logins HIPAA: vCenter Orchestrator Datastore Events HIPAA: vCenter Orchestrator Data Move HIPAA: vCenter Orchestrator Failed Logins HIPAA: vCenter Restart ESX Services HIPAA: vCenter Successful Logins HIPAA: vCloud Failed Logins HIPAA: vCloud Successful Logins HIPAA: vCloud User Created HIPAA: vCloud User Deleted or Removed HIPAA: VPN Users Accessing Corporate Network HIPAA: Web Access to Applications HIPAA: Web Access to Applications - F5 BIG-IP TMOS HIPAA: Web Access to Applications - Fortinet HIPAA: Web Access to Applications - PANOS HIPAA: Web Access to Applications - Microsoft IIS HIPAA: Windows New Services Installed **Compliance Suite Alerts** HIPAA: Accounts Created HIPAA: Accounts Deleted HIPAA: Cisco ISE, ACS Passwords Changed HIPAA: DB2 Database Configuration Change HIPAA: DB2 Database User Added or Dropped HIPAA: Groups Created HIPAA: Groups Deleted HIPAA: Groups Modified HIPAA: Guardium SQL Guard Config Changes HIPAA: Guardium SQL Guard Data Access

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		HIPAA: Guardium SQL Guard Logins
164.308(a)(4)(ii)(B)	Access Authorization (Addressable)	**Compliance Suite Alerts** (Cont.) HIPAA: HP NonStop Audit Configuration Changed HIPAA: HP NonStop Audit Permission Changed HIPAA: i5/OS Permission or Policy Change HIPAA: i5/OS Server or Service Status Change HIPAA: IBM AIX Password Changed HIPAA: Logins Failed HIPAA: Logins Succeeded HIPAA: LogLogic DSM Configuration Changes HIPAA: LogLogic DSM Data Access HIPAA: LogLogic DSM Logins HIPAA: LogLogic Management Center Passwords Changed HIPAA: LogLogic Universal Collector Configuration Changed HIPAA: Microsoft Operations Manager - Permissions Changed HIPAA: Microsoft Operations Manager - Windows Passwords Changed HIPAA: Microsoft Operations Manager - Windows Policies Changed HIPAA: Microsoft Sharepoint Content Deleted HIPAA: Microsoft Sharepoint Content Updated HIPAA: Microsoft Sharepoint Permission Changed HIPAA: Microsoft Sharepoint Policies Added, Removed, Modified HIPAA: NetApp Filer Audit Policies Changed HIPAA: Oracle Database Configuration Change HIPAA: Oracle Database Data Access HIPAA: Oracle Database Permissions Changed HIPAA: Oracle Database User Added or Deleted HIPAA: RACF Passwords Changed HIPAA: RACF Permissions Changed HIPAA: RACF Process Started HIPAA: Sybase ASE Database Config Changes HIPAA: Sybase ASE Database Data Access

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.308(a)(4)(ii)(B)	Access Authorization (Addressable)	**Compliance Suite Alerts** (Cont.) HIPAA: Symantec Endpoint Protection Policy Add, Delete, Modify HIPAA: TIBCO ActiveMatrix Administrator Permission Changed HIPAA: vCenter Orchestrator Login Failed HIPAA: vCenter Permission Change HIPAA: vCenter Restart ESX Services HIPAA: vCenter User Login Failed HIPAA: vCenter User Login Successful HIPAA: vCloud Director Login Failed HIPAA: vCloud Director Login Success HIPAA: vCloud User Created HIPAA: Windows Files Accessed HIPAA: Windows Passwords Changed HIPAA: Windows Permissions Changed HIPAA: Windows Policies Changed HIPAA: Windows Process Started

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.308(a)(4)(ii)(C)	Access Establishment and Modification (Addressable)	**Compliance Suite Reports** HIPAA: Accepted VPN Connections - RADIUS HIPAA: Account Activities on UNIX Servers HIPAA: Account Activities on Windows Servers HIPAA: Accounts Changed on NetApp Filer HIPAA: Accounts Changed on TIBCO Administrator HIPAA: Accounts Changed on TIBCO ActiveMatrix Administrator HIPAA: Accounts Changed on UNIX Servers HIPAA: Accounts Changed on Windows Servers HIPAA: Accounts Created on NetApp Filer HIPAA: Accounts Created on NetApp Filer Audit HIPAA: Accounts Created on Sidewinder HIPAA: Accounts Created on Symantec Endpoint Protection HIPAA: Accounts Created on TIBCO Administrator HIPAA: Accounts Created on TIBCO ActiveMatrix Administrator HIPAA: Accounts Created on UNIX Servers HIPAA: Accounts Created on Windows Servers HIPAA: Accounts Deleted on NetApp Filer HIPAA: Accounts Deleted on NetApp Filer Audit HIPAA: Accounts Deleted on Sidewinder HIPAA: Accounts Deleted on Symantec Endpoint Protection HIPAA: Accounts Deleted on TIBCO Administrator HIPAA: Accounts Deleted on TIBCO ActiveMatrix Administrator HIPAA: Accounts Deleted on UNIX Servers HIPAA: Accounts Deleted on Windows Servers HIPAA: Check Point Management Station Login HIPAA: Cisco ISE, ACS Accounts Created HIPAA: Cisco ISE, ACS Accounts Removed HIPAA: Cisco ISE, ACS Password Changes HIPAA: Creation and Deletion of System Level Objects: DB2 Database

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		HIPAA: Creation and Deletion of System Level Objects: Oracle

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.308(a)(4)(ii)(C)	Access Establishment and Modification (Addressable)	Compliance Suite Reports (Cont.) HIPAA: Creation and Deletion of System Level Objects: SQL Server HIPAA: Creation and Deletion of System Level Objects: Windows HIPAA: DB2 Database Configuration Changes HIPAA: DB2 Database Failed Logins HIPAA: DB2 Database Successful Logins HIPAA: DB2 Database User Additions and Deletions HIPAA: Denied VPN Connections - RADIUS HIPAA: DHCP Granted/Renewed Activities on Microsoft DHCP HIPAA: DHCP Granted/Renewed Activities on VMware vShield HIPAA: ESX Accounts Activities HIPAA: ESX Accounts Created HIPAA: ESX Accounts Deleted HIPAA: ESX Failed Logins HIPAA: ESX Group Activities HIPAA: ESX Logins Failed Unknown User HIPAA: ESX Logins Succeeded HIPAA: F5 BIG-IP TMOS Login Failed HIPAA: F5 BIG-IP TMOS Login Successful HIPAA: F5 BIG-IP TMOS Password Changes HIPAA: Failed Logins HIPAA: Group Activities on UNIX Servers HIPAA: Group Activities on Windows Servers HIPAA: Guardium SQL Guard Audit Configuration Changes HIPAA: Guardium SQL Guard Audit Data Access HIPAA: Guardium SQL Guard Audit Logins HIPAA: Guardium SQL Guard Configuration Changes HIPAA: Guardium SQL Guard Data Access HIPAA: Guardium SQL Guard Logins HIPAA: Group Activities on NetApp Filer Audit

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		HIPAA: Group Activities on Symantec Endpoint Protection

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.308(a)(4)(ii)(C)	Access Establishment and Modification (Addressable)	**Compliance Suite Reports** (Cont.) HIPAA: Group Activities on TIBCO ActiveMatrix Administrator HIPAA: HP NonStop Audit Configuration Changes HIPAA: HP NonStop Audit Login Failed HIPAA: HP NonStop Audit Login Successful HIPAA: HP NonStop Audit Object Changes HIPAA: HP NonStop Audit Permissions Changed HIPAA: i5/OS DST Password Reset HIPAA: i5/OS Network User Login Failed HIPAA: i5/OS Network User Login Successful HIPAA: i5/OS Network User Profile Creation HIPAA: i5/OS Network User Profile Deletion HIPAA: i5/OS Network User Profile Modified HIPAA: i5/OS Object Permissions Modified HIPAA: i5/OS User Login Failed HIPAA: i5/OS User Login Successful HIPAA: i5/OS User Profile Creation HIPAA: i5/OS User Profile Modifications HIPAA: Juniper SSL VPN Successful Logins by IP HIPAA: Juniper SSL VPN Successful Logins by User HIPAA: Juniper SSL VPN (Secure Access) Successful Logins by IP HIPAA: Juniper SSL VPN (Secure Access) Successful Logins by User HIPAA: LogLogic DSM Configuration Changes HIPAA: LogLogic DSM Data Access HIPAA: LogLogic DSM Logins HIPAA: LogLogic Management Center Account Activities HIPAA: LogLogic Management Center Login HIPAA: LogLogic Management Center Password Changes HIPAA: LogLogic Universal Collector Configuration Changes HIPAA: Microsoft Operations Manager - Windows Accounts Activities

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.308(a)(4)(ii)(C)	Access Establishment and Modification (Addressable)	**Compliance Suite Reports** (Cont.) HIPAA: Microsoft Operations Manager - Windows Accounts Created HIPAA: Microsoft Operations Manager - Windows Password Changes HIPAA: Microsoft Operations Manager - Windows Permissions Modified HIPAA: Microsoft Operations Manager - Windows Policies Modified HIPAA: Microsoft Sharepoint Content Deleted HIPAA: Microsoft Sharepoint Content Updates HIPAA: Microsoft Sharepoint Permissions Changed HIPAA: Microsoft Sharepoint Policy Add, Remove, or Modify HIPAA: Microsoft SQL Server Configuration Changes HIPAA: Microsoft SQL Server Data Access HIPAA: Microsoft SQL Server Database Failed Logins HIPAA: Microsoft SQL Server Database Successful Logins HIPAA: Microsoft SQL Server Database Permission Events HIPAA: Microsoft SQL Server Database User Additions and Deletions HIPAA: Microsoft SQL Server Password Changes HIPAA: NetApp Filer Audit Login Failed HIPAA: NetApp Filer Audit Login Successful HIPAA: NetApp Filer Login Failed HIPAA: NetApp Filer Login Successful HIPAA: NetApp Filer Password Changes HIPAA: Oracle Database Configuration Changes HIPAA: Oracle Database Data Access HIPAA: Oracle Database Failed Logins HIPAA: Oracle Database Successful Logins HIPAA: Oracle Database Permission Events HIPAA: Oracle Database User Additions and Deletions HIPAA: RACF Accounts Created

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		HIPAA: RACF Accounts Deleted HIPAA: RACF Accounts Modified

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.308(a)(4)(ii)(C)	Access Establishment and Modification (Addressable)	**Compliance Suite Reports** (Cont.) HIPAA: RACF Failed Logins HIPAA: RACF Password Changed HIPAA: RACF Permissions Changed HIPAA: RACF Successful Logins HIPAA: Password Changes on Windows Servers HIPAA: Permissions Modified on Windows Servers HIPAA: Policies Modified on Windows Servers HIPAA: Successful Logins HIPAA: Sybase ASE Database Configuration Changes HIPAA: Sybase ASE Database Data Access HIPAA: Sybase ASE Database User Additions and Deletions HIPAA: Sybase ASE Failed Logins HIPAA: Sybase ASE Successful Logins HIPAA: Symantec Endpoint Protection Password Changes HIPAA: TIBCO Administrator Password Changes HIPAA: TIBCO Administrator Permission Changes HIPAA: TIBCO ActiveMatrix Administrator Failed Logins HIPAA: TIBCO ActiveMatrix Administrator Permission Changes HIPAA: TIBCO ActiveMatrix Administrator Successful Logins HIPAA: UNIX Failed Logins HIPAA: vCenter Failed Logins HIPAA: vCenter Orchestrator Failed Logins HIPAA: vCenter Successful Logins HIPAA: vCenter User Permission Change HIPAA: vCloud Failed Logins HIPAA: vCloud Successful Logins HIPAA: vCloud User Created HIPAA: vCloud User Deleted or Removed HIPAA: VPN Users Accessing Corporate Network

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.308(a)(4)(ii)(C)	Access Establishment and Modification (Addressable)	**Compliance Suite Alerts** HIPAA: Accounts Created HIPAA: Accounts Deleted HIPAA: Accounts Modified HIPAA: Cisco ISE, ACS Passwords Changed HIPAA: DB2 Database Configuration Change HIPAA: DB2 Database User Added or Dropped HIPAA: Groups Created HIPAA: Groups Deleted HIPAA: Groups Modified HIPAA: Guardium SQL Guard Config Changes HIPAA: Guardium SQL Guard Data Access HIPAA: Guardium SQL Guard Logins HIPAA: HP NonStop Audit Configuration Changed HIPAA: HP NonStop Audit Permission Changed HIPAA: i5/OS Network Profile Changes HIPAA: i5/OS Permission or Policy Change HIPAA: i5/OS User Profile Changes HIPAA: IBM AIX Password Changed HIPAA: Logins Failed HIPAA: Logins Succeeded HIPAA: LogLogic DSM Configuration Changes HIPAA: LogLogic DSM Data Access HIPAA: LogLogic DSM Logins HIPAA: LogLogic Management Center Passwords Changed HIPAA: LogLogic Universal Collector Configuration Changed HIPAA: Microsoft Operations Manager - Permissions Changed HIPAA: Microsoft Operations Manager - Windows Passwords Changed HIPAA: Microsoft Operations Manager - Windows Policies Changed HIPAA: Microsoft Sharepoint Content Deleted

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.308(a)(4)(ii)(C)	Access Establishment and Modification (Addressable)	**Compliance Suite Alerts** (Cont.) HIPAA: Microsoft Sharepoint Content Updated HIPAA: Microsoft Sharepoint Permission Changed HIPAA: Microsoft Sharepoint Policies Added, Removed, Modified HIPAA: NetApp Authentication Failure HIPAA: NetApp Filer Audit Policies Changed HIPAA: Oracle Database Configuration Change HIPAA: Oracle Database Data Access HIPAA: Oracle Database Permissions Changed HIPAA: Oracle Database User Added or Deleted HIPAA: RACF Passwords Changed HIPAA: RACF Permissions Changed HIPAA: Sybase ASE Database Config Changes HIPAA: Sybase ASE Database Data Access HIPAA: Symantec Endpoint Protection Policy Add, Delete, Modify HIPAA: TIBCO ActiveMatrix Administrator Permission Changed HIPAA: vCenter Orchestrator Login Failed HIPAA: vCenter Permission Change HIPAA: vCenter User Login Failed HIPAA: vCenter User Login Successful HIPAA: vCloud Director Login Failed HIPAA: vCloud Director Login Success HIPAA: vCloud User Created HIPAA: Windows Passwords Changed HIPAA: Windows Permissions Changed HIPAA: Windows Policies Changed

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.308(a)(5)(ii)(A)	Security Reminders (Addressable)	**Compliance Suite Reports** HIPAA: Cisco ESA: Updated HIPAA: LogLogic Management Center Upgrade Success HIPAA: Software Update Successes on i5/OS HIPAA: Symantec AntiVirus: Updated HIPAA: Symantec Endpoint Protection: Updated HIPAA: Windows Software Update Activities HIPAA: Windows Software Update Failures HIPAA: Windows Software Update Successes **Compliance Suite Alerts** HIPAA: i5/OS Software Updates HIPAA: LogLogic Management Center Upgrade Succeeded HIPAA: Windows Software Updates HIPAA: Windows Software Updates Failed HIPAA: Windows Software Updates Succeeded

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.308(a)(5)(ii)(C)	Log-In Monitoring (Addressable)	**Compliance Suite Reports** HIPAA: Accepted VPN Connections - RADIUS HIPAA: Check Point Management Station Login HIPAA: DB2 Database Failed Logins HIPAA: DB2 Database Successful Logins HIPAA: Denied VPN Connections - RADIUS HIPAA: ESX Failed Logins HIPAA: ESX Logins Failed Unknown User HIPAA: ESX Logins Succeeded HIPAA: F5 BIG-IP TMOS Login Failed HIPAA: F5 BIG-IP TMOS Login Successful HIPAA: Failed Logins HIPAA: Guardium SQL Guard Audit Logins HIPAA: Guardium SQL Guard Logins HIPAA: HP NonStop Audit Login Failed HIPAA: HP NonStop Audit Login Successful HIPAA: i5/OS Network User Login Failed HIPAA: i5/OS Network User Login Successful HIPAA: i5/OS User Login Failed HIPAA: i5/OS User Login Successful HIPAA: Juniper SSL VPN Successful Logins by IP HIPAA: Juniper SSL VPN Successful Logins by User HIPAA: Juniper SSL VPN (Secure Access) Successful Logins by IP HIPAA: Juniper SSL VPN (Secure Access) Successful Logins by User HIPAA: LogLogic DSM Logins HIPAA: LogLogic Management Center Login HIPAA: Microsoft SQL Server Database Failed Logins HIPAA: Microsoft SQL Server Database Successful Logins HIPAA: NetApp Filer Audit Login Failed HIPAA: NetApp Filer Audit Login Successful HIPAA: NetApp Filer Login Failed HIPAA: NetApp Filer Login Successful

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.308(a)(5)(ii)(C)	Log-In Monitoring (Addressable)	**Compliance Suite Reports** (Cont.) HIPAA: Oracle Database Failed Logins HIPAA: Oracle Database Successful Logins HIPAA: RACF Failed Logins HIPAA: RACF Successful Logins HIPAA: Successful Logins HIPAA: Sybase ASE Failed Logins HIPAA: Sybase ASE Successful Logins HIPAA: TIBCO ActiveMatrix Administrator Failed Logins HIPAA: TIBCO ActiveMatrix Administrator Successful Logins HIPAA: Unauthorized Logins HIPAA: UNIX Failed Logins HIPAA: vCenter Failed Logins HIPAA: vCenter Orchestrator Failed Logins HIPAA: vCenter Successful Logins HIPAA: vCloud Failed Logins HIPAA: vCloud Successful Logins HIPAA: VPN Users Accessing Corporate Network **Compliance Suite Alerts** HIPAA: Guardium SQL Guard Logins HIPAA: Logins Failed HIPAA: Logins Succeeded HIPAA: LogLogic DSM Logins HIPAA: vCenter Orchestrator Login Failed HIPAA: vCenter User Login Failed HIPAA: vCenter User Login Successful HIPAA: vCloud Director Login Failed HIPAA: vCloud Director Login Success

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.308(a)(5)(ii)(D)	Password Management (Addressable)	**Compliance Suite Reports** HIPAA: Cisco ISE, ACS Password Changes HIPAA: F5 BIG-IP TMOS Password Changes HIPAA: i5/OS DST Password Reset HIPAA: LogLogic Management Center Password Changes HIPAA: Microsoft Operations Manager - Windows Password Changes HIPAA: NetApp Filer Password Changes HIPAA: Password Changes on Windows Servers HIPAA: RACF Password Changed HIPAA: Symantec Endpoint Protection Password Changes HIPAA: TIBCO Administrator Password Changes **Compliance Suite Alerts** HIPAA: Cisco ISE, ACS Passwords Changed HIPAA: IBM AIX Password Changed HIPAA: LogLogic Management Center Passwords Changed HIPAA: Microsoft Operations Manager - Windows Passwords Changed HIPAA: RACF Passwords Changed HIPAA: Windows Passwords Changed

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.308(a)(6)(ii)	Response and Reporting (Required)	**Compliance Suite Reports** HIPAA: Applications Under Attack HIPAA: Applications Under Attack - Cisco IOS HIPAA: Applications Under Attack - ISS SiteProtector HIPAA: Applications Under Attack - SiteProtector HIPAA: Applications Under Attack - Sourcefire Defense Center HIPAA: Attacks Detected HIPAA: Attack Origins HIPAA: Attack Origins - Cisco IOS HIPAA: Attack Origins - HIPS HIPAA: Attack Origins - ISS SiteProtector HIPAA: Attack Origins - SiteProtector HIPAA: Attack Origins - Sourcefire Defense Center HIPAA: Attacks Detected - Cisco IOS HIPAA: Attacks Detected - HIPS HIPAA: Attacks Detected - ISS SiteProtector HIPAA: Attacks Detected - SiteProtector HIPAA: Attacks Detected - Sourcefire Defense Center HIPAA: Cisco ESA: Attacks by Event ID HIPAA: Cisco ESA: Attacks Detected HIPAA: Cisco ESA: Attacks by Threat Name HIPAA: Cisco ESA: Scans HIPAA: Cisco ESA: Updated HIPAA: FortiOS: Attacks by Event ID HIPAA: FortiOS: Attacks by Threat Name HIPAA: FortiOS: Attacks Detected HIPAA: FortiOS DLP Attacks Detected HIPAA: McAfee AntiVirus: Attacks by Event ID HIPAA: McAfee AntiVirus: Attacks by Threat Name HIPAA: McAfee AntiVirus: Attacks Detected HIPAA: PANOS: Attacks by Event ID HIPAA: PANOS: Attacks by Threat Name HIPAA: PANOS: Attacks Detected

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		HIPAA: Symantec AntiVirus: Attacks by Threat Name HIPAA: Applications Under Attack - FireEye MPS
164.308(a)(6)(ii)	Response and Reporting (Required)	**Compliance Suite Reports** (Cont.) HIPAA: Symantec AntiVirus: Attacks Detected HIPAA: Symantec AntiVirus: Scans HIPAA: Symantec AntiVirus: Updated HIPAA: Symantec Endpoint Protection: Attacks by Threat Name HIPAA: Symantec Endpoint Protection: Attacks Detected HIPAA: Symantec Endpoint Protection: Scans HIPAA: Symantec Endpoint Protection: Updated HIPAA: TrendMicro OfficeScan: Attacks Detected HIPAA: TrendMicro OfficeScan: Attacks Detected by Threat Name HIPAA: TrendMicro Control Manager: Attacks Detected HIPAA: TrendMicro Control Manager: Attacks Detected by Threat Name Compliance Suite Alert HIPAA: Anomalous IDS Alerts
164.308(a)(7)(ii)(A)	Data Backup Plan (Required)	**Compliance Suite Reports** HIPAA: NetApp Filer Snapshot Error **Compliance Suite Alerts** HIPAA: NetApp Filer Disk Failure HIPAA: NetApp Filer Disk Missing HIPAA: NetApp Filer Disk Inserted HIPAA: NetApp Filer Disk Pulled HIPAA: NetApp Filer Snapshot Error

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.308(a)(7)(ii)(B)	Disaster Recovery Plan (Required)	**Compliance Suite Reports** HIPAA: NetApp Filer Snapshot Error **Compliance Suite Alerts** HIPAA: NetApp Filer Disk Failure HIPAA: NetApp Filer Disk Missing HIPAA: NetApp Filer Disk Inserted HIPAA: NetApp Filer Disk Pulled HIPAA: NetApp Filer Snapshot Error

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.308(a)(7)(ii)(C)	Emergency Mode Operational plan (Required)	**Compliance Suite Reports** HIPAA: Accepted VPN Connections - RADIUS HIPAA: Account Activities on UNIX Servers HIPAA: Account Activities on Windows Servers HIPAA: Accounts Created on NetApp Filer HIPAA: Accounts Created on NetApp Filer Audit HIPAA: Accounts Created on Sidewinder HIPAA: Accounts Created on Symantec Endpoint Protection HIPAA: Accounts Created on TIBCO ActiveMatrix Administrator HIPAA: Accounts Created on TIBCO Administrator HIPAA: Accounts Created on UNIX Servers HIPAA: Accounts Created on Windows Servers HIPAA: Accounts Deleted on NetApp Filer HIPAA: Accounts Deleted on NetApp Filer Audit HIPAA: Accounts Deleted on Sidewinder HIPAA: Accounts Deleted on Symantec Endpoint Protection HIPAA: Accounts Deleted on TIBCO Administrator HIPAA: Accounts Deleted on TIBCO ActiveMatrix Administrator HIPAA: Accounts Deleted on UNIX Servers HIPAA: Accounts Deleted on Windows Servers HIPAA: Check Point Management Station Login HIPAA: Cisco ISE, ACS Accounts Created HIPAA: Cisco ISE, ACS Accounts Removed HIPAA: DB2 Database Successful Logins HIPAA: ESX Accounts Activities HIPAA: ESX Accounts Created HIPAA: ESX Accounts Deleted HIPAA: ESX Logins Succeeded HIPAA: F5 BIG-IP TMOS Login Successful HIPAA: Guardium SQL Guard Audit Logins HIPAA: Guardium SQL Guard Logins HIPAA: HP NonStop Audit Login Successful

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.308(a)(7)(ii)(C)	Emergency Mode Operational plan (Required)	**Compliance Suite Reports** (Cont.) HIPAA: i5/OS Network User Login Successful HIPAA: i5/OS Network User Profile Creation HIPAA: i5/OS Network User Profile Deletion HIPAA: i5/OS User Login Successful HIPAA: i5/OS User Profile Creation HIPAA: Juniper SSL VPN Successful Logins by IP HIPAA: Juniper SSL VPN Successful Logins by User HIPAA: Juniper SSL VPN (Secure Access) Successful Logins by IP HIPAA: Juniper SSL VPN (Secure Access) Successful Logins by User HIPAA: LogLogic DSM Logins HIPAA: LogLogic Management Center Account Activities HIPAA: LogLogic Management Center Login HIPAA: Microsoft Operations Manager - Windows Accounts Activities HIPAA: Microsoft Operations Manager - Windows Accounts Created HIPAA: Microsoft SQL Server Database Successful Logins HIPAA: NetApp Filer Audit Login Successful HIPAA: NetApp Filer Login Successful HIPAA: Oracle Database Successful Logins HIPAA: RACF Accounts Created HIPAA: RACF Accounts Deleted HIPAA: RACF Successful Logins HIPAA: Successful Logins HIPAA: Sybase ASE Successful Logins HIPAA: TIBCO ActiveMatrix Administrator Successful Logins HIPAA: vCenter Successful Logins

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.308(a)(7)(ii)(C)	Emergency Mode Operational plan (Required)	**Compliance Suite Reports** (Cont.) HIPAA: vCloud Successful Logins HIPAA: vCloud User Created HIPAA: vCloud User Deleted or Removed HIPAA: VPN Users Accessing Corporate Network **Compliance Suite Alerts** HIPAA: Accounts Created HIPAA: Accounts Deleted HIPAA: Guardium SQL Guard Logins HIPAA: Logins Succeeded HIPAA: LogLogic DSM Logins HIPAA: vCenter User Login Successful HIPAA: vCloud Director Login Success HIPAA: vCloud User Created
164.308(a)(7)(ii)(D)	Testing and Revision Procedures (Addressable)	**Compliance Suite Reports** HIPAA: NetApp Filer Snapshot Error Compliance Suite Alerts HIPAA: NetApp Filer Disk Failure HIPAA: NetApp Filer Disk Missing HIPAA: NetApp Filer Disk Inserted HIPAA: NetApp Filer Disk Pulled HIPAA: NetApp Filer Snapshot Error

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.312(a)(2)(i)	Unique User Identification (Required)	**Compliance Suite Reports** HIPAA: Accepted VPN Connections - RADIUS HIPAA: Account Activities on UNIX Servers HIPAA: Account Activities on Windows Servers HIPAA: Accounts Created on NetApp Filer HIPAA: Accounts Created on NetApp Filer Audit HIPAA: Accounts Created on Sidewinder HIPAA: Accounts Created on Symantec Endpoint Protection HIPAA: Accounts Created on TIBCO Administrator HIPAA: Accounts Created on TIBCO ActiveMatrix Administrator HIPAA: Accounts Created on UNIX Servers HIPAA: Accounts Created on Windows Servers HIPAA: Accounts Deleted on NetApp Filer HIPAA: Accounts Deleted on NetApp Filer Audit HIPAA: Accounts Deleted on Sidewinder HIPAA: Accounts Deleted on Symantec Endpoint Protection HIPAA: Accounts Deleted on TIBCO Administrator HIPAA: Accounts Deleted on TIBCO ActiveMatrix Administrator HIPAA: Accounts Deleted on UNIX Servers HIPAA: Accounts Deleted on Windows Servers HIPAA: Check Point Management Station Login HIPAA: Cisco ISE, ACS Accounts Created HIPAA: Cisco ISE, ACS Accounts Removed HIPAA: DB2 Database Failed Logins HIPAA: DB2 Database Successful Logins HIPAA: Denied VPN Connections - RADIUS HIPAA: DHCP Granted/Renewed Activities on Microsoft DHCP HIPAA: DHCP Granted/Renewed Activities on VMware vShield HIPAA: ESX Accounts Activities HIPAA: ESX Accounts Created

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		HIPAA: Pulse Connect Secure Successful Logins by IP

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.312(a)(2)(i)	Unique User Identification (Required)	**Compliance Suite reports** (Cont.) HIPAA: ESX Accounts Deleted HIPAA: ESX Failed Logins HIPAA: ESX Logins Failed Unknown User HIPAA: ESX Logins Succeeded HIPAA: F5 BIG-IP TMOS Login Failed HIPAA: F5 BIG-IP TMOS Login Successful HIPAA: Failed Logins HIPAA: Guardium SQL Guard Audit Logins HIPAA: Guardium SQL Guard Logins HIPAA: HP NonStop Audit Login Failed HIPAA: HP NonStop Audit Login Successful HIPAA: i5/OS Network User Login Failed HIPAA: i5/OS Network User Login Successful HIPAA: i5/OS Network User Profile Creation HIPAA: i5/OS Network User Profile Deletion HIPAA: i5/OS User Login Failed HIPAA: i5/OS User Login Successful HIPAA: i5/OS User Profile Creation HIPAA: Juniper SSL VPN Successful Logins by IP HIPAA: Juniper SSL VPN Successful Logins by User HIPAA: Juniper SSL VPN (Secure Access) Successful Logins by IP HIPAA: Juniper SSL VPN (Secure Access) Successful Logins by User HIPAA: LogLogic DSM Logins HIPAA: LogLogic Management Center Account Activities HIPAA: LogLogic Management Center Login HIPAA: Microsoft Operations Manager - Windows Accounts Activities HIPAA: Microsoft Operations Manager - Windows Accounts Created HIPAA: Microsoft SQL Server Database Failed Logins HIPAA: Microsoft SQL Server Database Successful Logins

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.312(a)(2)(i)	Unique User Identification (Required)	**Compliance Suite Reports** (Cont.) HIPAA: NetApp Filer Audit Login Failed HIPAA: NetApp Filer Audit Login Successful HIPAA: NetApp Filer Login Failed HIPAA: NetApp Filer Login Successful HIPAA: Oracle Database Failed Logins HIPAA: Oracle Database Successful Logins HIPAA: RACF Accounts Created HIPAA: RACF Accounts Deleted HIPAA: RACF Failed Logins HIPAA: RACF Successful Logins HIPAA: Successful Logins HIPAA: Sybase ASE Failed Logins HIPAA: Sybase ASE Successful Logins HIPAA: TIBCO ActiveMatrix Administrator Failed Logins HIPAA: TIBCO ActiveMatrix Administrator Successful Logins HIPAA: UNIX Failed Logins HIPAA: vCenter Failed Logins HIPAA: vCenter Orchestrator Failed Logins HIPAA: vCenter Successful Logins HIPAA: vCloud Failed Logins HIPAA: vCloud Successful Logins HIPAA: vCloud User Created HIPAA: vCloud User Deleted or Removed HIPAA: VPN Users Accessing Corporate Network **Compliance Suite Alerts** HIPAA: Accounts Created HIPAA: Accounts Deleted HIPAA: Guardium SQL Guard Logins HIPAA: Logins Succeeded HIPAA: Logins Failed HIPAA: LogLogic DSM Logins HIPAA: vCenter User Login Failed

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		Compliance Suite Alerts (Cont.) HIPAA: vCenter User Login Successful HIPAA: vCenter Orchestrator Login Failed HIPAA: vCloud Director Login Failed HIPAA: vCloud Director Login Success HIPAA: vCloud User Created

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.312(a)(2)(ii)	Emergency Access Procedure (Required)	**Compliance Suite Reports** HIPAA: Accepted VPN Connections - RADIUS HIPAA: Account Activities on UNIX Servers HIPAA: Account Activities on Windows Servers HIPAA: Accounts Created on NetApp Filer HIPAA: Accounts Created on NetApp Filer Audit HIPAA: Accounts Created on Sidewinder HIPAA: Accounts Created on Symantec Endpoint Protection HIPAA: Accounts Created on TIBCO Administrator HIPAA: Accounts Created on TIBCO ActiveMatrix Administrator HIPAA: Accounts Created on UNIX Servers HIPAA: Accounts Created on Windows Servers HIPAA: Accounts Deleted on NetApp Filer HIPAA: Accounts Deleted on NetApp Filer Audit HIPAA: Accounts Deleted on Sidewinder HIPAA: Accounts Deleted on Symantec Endpoint Protection HIPAA: Accounts Deleted on TIBCO Administrator HIPAA: Accounts Deleted on TIBCO ActiveMatrix Administrator HIPAA: Accounts Deleted on UNIX Servers HIPAA: Accounts Deleted on Windows Servers HIPAA: Check Point Management Station Login HIPAA: Cisco ISE, ACS Accounts Created HIPAA: Cisco ISE, ACS Accounts Removed HIPAA: DB2 Database Successful Logins HIPAA: ESX Accounts Activities HIPAA: ESX Accounts Created HIPAA: ESX Accounts Deleted HIPAA: ESX Logins Succeeded HIPAA: F5 BIG-IP TMOS Login Successful HIPAA: Guardium SQL Guard Audit Logins

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.312(a)(2)(ii)	Emergency Access Procedure (Required)	**Compliance Suite Reports** (Cont.) HIPAA: i5/OS Network User Profile Deletion HIPAA: i5/OS User Login Successful HIPAA: Guardium SQL Guard Logins HIPAA: HP NonStop Audit Login Successful HIPAA: i5/OS Network User Login Successful HIPAA: i5/OS Network User Profile Creation HIPAA: i5/OS User Profile Creation HIPAA: Juniper SSL VPN Successful Logins by IP HIPAA: Juniper SSL VPN Successful Logins by User HIPAA: Juniper SSL VPN (Secure Access) Successful Logins by IP HIPAA: Juniper SSL VPN (Secure Access) Successful Logins by User HIPAA: LogLogic DSM Logins HIPAA: LogLogic Management Center Account Activities HIPAA: LogLogic Management Center Login HIPAA: Microsoft Operations Manager - Windows Accounts Activities HIPAA: Microsoft Operations Manager - Windows Accounts Created HIPAA: Microsoft SQL Server Database Successful Logins HIPAA: Oracle Database Successful Logins HIPAA: NetApp Filer Audit Login Successful HIPAA: NetApp Filer Login Successful HIPAA: RACF Accounts Created HIPAA: RACF Accounts Deleted HIPAA: RACF Successful Logins HIPAA: Successful Logins HIPAA: Sybase ASE Successful Logins HIPAA: TIBCO ActiveMatrix Administrator Successful Logins HIPAA: vCenter Successful Logins HIPAA: vCloud Successful Logins HIPAA: vCloud User Created

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		HIPAA: vCloud User Deleted or Removed
164.312(a)(2)(ii)	Emergency Access Procedure (Required)	**Compliance Suite Alerts** HIPAA: VPN Users Accessing Corporate Network HIPAA: Accounts Created HIPAA: Accounts Deleted HIPAA: Guardium SQL Guard Logins HIPAA: Logins Succeeded HIPAA: LogLogic DSM Logins HIPAA: vCenter User Login Successful HIPAA: vCloud Director Login Success HIPAA: vCloud User Created
164.312(a)(2)(iii)	Automatic Logoff (Addressable)	**Compliance Suite Reports** HIPAA: Account Activities on UNIX Servers HIPAA: Account Activities on Windows Servers HIPAA: Active Directory System Changes HIPAA: Check Point Management Station Logout HIPAA: ESX Accounts Activities HIPAA: LogLogic Management Center Account Activities HIPAA: Microsoft Operations Manager - Windows Accounts Activities HIPAA: Microsoft Operations Manager - Windows Policies Modified HIPAA: Microsoft Sharepoint Policy Add, Remove, or Modify HIPAA: Policies Modified on Windows Servers **Compliance Suite Alerts** HIPAA: Active Directory Changes HIPAA: Microsoft Operations Manager - Windows Policies Changed HIPAA: Microsoft Sharepoint Policies Added, Removed, Modified HIPAA: NetApp Filer Audit Policies Changed HIPAA: Symantec Endpoint Protection Policy Add, Delete, Modify HIPAA: Windows Policies Changed

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.312(b)	Audit Controls (Required)	**Compliance Suite Reports** HIPAA: DNS Server Error HIPAA: LogLogic Disk Full HIPAA: LogLogic File Retrieval Errors HIPAA: LogLogic Message Routing Errors HIPAA: NetApp Filer Audit Logs Cleared HIPAA: Windows Audit Logs Cleared **Compliance Suite Alerts** HIPAA: LogLogic Disk Full HIPAA: LogLogic File Retrieval Errors HIPAA: LogLogic Message Routing Errors HIPAA: NetApp Filer File System Full HIPAA: Windows Audit Log Cleared

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.312(c)(2)	Mechanism to Authenticate Electronic Protected Health Information (Addressable)	**Compliance Suite Reports** HIPAA: Accepted VPN Connections - RADIUS HIPAA: Account Activities on UNIX Servers HIPAA: Account Activities on Windows Servers HIPAA: Accounts Created on NetApp Filer HIPAA: Accounts Created on NetApp Filer Audit HIPAA: Accounts Created on Sidewinder HIPAA: Accounts Created on Symantec Endpoint Protection HIPAA: Accounts Created on TIBCO Administrator HIPAA: Accounts Created on TIBCO ActiveMatrix Administrator HIPAA: Accounts Created on UNIX Servers HIPAA: Accounts Created on Windows Servers HIPAA: Accounts Deleted on NetApp Filer HIPAA: Accounts Deleted on NetApp Filer Audit HIPAA: Accounts Deleted on Sidewinder HIPAA: Accounts Deleted on Symantec Endpoint Protection HIPAA: Accounts Deleted on TIBCO Administrator HIPAA: Accounts Deleted on TIBCO ActiveMatrix Administrator HIPAA: Accounts Deleted on UNIX Servers HIPAA: Accounts Deleted on Windows Servers HIPAA: Active Directory System Changes HIPAA: Check Point Management Station Login HIPAA: Cisco ISE, ACS Accounts Created HIPAA: Cisco ISE, ACS Accounts Removed HIPAA: Cisco ISE, ACS Password Changes HIPAA: DB2 Database Failed Logins HIPAA: DB2 Database Successful Logins HIPAA: Denied VPN Connections - RADIUS HIPAA: ESX Accounts Activities HIPAA: ESX Accounts Created HIPAA: ESX Accounts Deleted HIPAA: ESX Failed Logins HIPAA: ESX Group Activities

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		HIPAA: Pulse Connect Secure Successful Logins by IP

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.312(c)(2)	Mechanism to Authenticate Electronic Protected Health Information (Addressable)	**Compliance Suite Reports** (Cont.) HIPAA: ESX Logins Failed Unknown User HIPAA: ESX Logins Succeeded HIPAA: F5 BIG-IP TMOS Login Failed HIPAA: F5 BIG-IP TMOS Login Successful HIPAA: F5 BIG-IP TMOS Password Changes HIPAA: Failed Logins HIPAA: Group Activities on NetApp Filer Audit HIPAA: Group Activities on Symantec Endpoint Protection HIPAA: Group Activities on TIBCO ActiveMatrix Administrator HIPAA: Group Activities on UNIX Servers HIPAA: Group Activities on Windows Servers HIPAA: Guardium SQL Guard Audit Logins HIPAA: Guardium SQL Guard Logins HIPAA: HP NonStop Audit Login Failed HIPAA: HP NonStop Audit Login Successful HIPAA: HP NonStop Audit Permissions Changed HIPAA: i5/OS DST Password Reset HIPAA: i5/OS Network User Login Failed HIPAA: i5/OS Network User Login Successful HIPAA: i5/OS Network User Profile Creation HIPAA: i5/OS Network User Profile Deletion HIPAA: i5/OS Object Permissions Modified HIPAA: i5/OS User Login Failed HIPAA: i5/OS User Login Successful HIPAA: i5/OS User Profile Creation HIPAA: Juniper SSL VPN Successful Logins by IP HIPAA: Juniper SSL VPN Successful Logins by User HIPAA: Juniper SSL VPN (Secure Access) Successful Logins by IP HIPAA: Juniper SSL VPN (Secure Access) Successful Logins by User HIPAA: LogLogic DSM Logins HIPAA: LogLogic Management Center Account Activities

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.312(c)(2)	Mechanism to Authenticate Electronic Protected Health Information (Addressable)	**Compliance Suite Reports** (Cont.) HIPAA: LogLogic Management Center Login HIPAA: LogLogic Management Center Password Changes HIPAA: Microsoft Operations Manager - Windows Accounts Activities HIPAA: Microsoft Operations Manager - Windows Accounts Created HIPAA: Microsoft Operations Manager - Windows Password Changes HIPAA: Microsoft Operations Manager - Windows Permissions Modified HIPAA: Microsoft Sharepoint Permissions Changed HIPAA: Microsoft SQL Server Database Failed Logins HIPAA: Microsoft SQL Server Database Successful Logins HIPAA: NetApp Filer Audit Login Failed HIPAA: NetApp Filer Audit Login Successful HIPAA: NetApp Filer Login Failed HIPAA: NetApp Filer Login Successful HIPAA: NetApp Filer Password Changes HIPAA: Oracle Database Failed Logins HIPAA: Oracle Database Successful Logins HIPAA: Password Changes on Windows Servers HIPAA: Permissions Modified on Windows Servers HIPAA: RACF Accounts Created HIPAA: RACF Accounts Deleted HIPAA: RACF Failed Logins HIPAA: RACF Password Changed HIPAA: RACF Permissions Changed HIPAA: RACF Successful Logins HIPAA: Successful Logins HIPAA: Sybase ASE Failed Logins HIPAA: Sybase ASE Successful Logins HIPAA: Symantec Endpoint Protection Password Changes

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		HIPAA: TIBCO ActiveMatrix Administrator Successful Logins

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.312(c)(2)	Mechanism to Authenticate Electronic Protected Health Information (Addressable)	**Compliance Suite Reports** (Cont.) HIPAA: TIBCO Administrator Password Changes HIPAA: TIBCO Administrator Permission Changes HIPAA: TIBCO ActiveMatrix Administrator Failed Logins HIPAA: TIBCO ActiveMatrix Administrator Permission Changes HIPAA: UNIX Failed Logins HIPAA: vCenter Failed Logins HIPAA: vCenter Orchestrator Failed Logins HIPAA: vCenter Successful Logins HIPAA: vCenter User Permission Change HIPAA: vCloud Failed Logins HIPAA: vCloud Successful Logins HIPAA: vCloud User Created HIPAA: vCloud User Deleted or Removed HIPAA: VPN Users Accessing Corporate Network **Compliance Suite Alerts** HIPAA: Accounts Created HIPAA: Accounts Deleted HIPAA: Active Directory Changes HIPAA: Cisco ISE, ACS Passwords Changed HIPAA: Groups Created HIPAA: Group Members Added HIPAA: Guardium SQL Guard Logins HIPAA: HP NonStop Audit Permission Changed HIPAA: i5/OS Permission or Policy Change HIPAA: IBM AIX Password Changed HIPAA: LogLogic DSM Logins HIPAA: Logins Succeeded HIPAA: Logins Failed HIPAA: LogLogic Management Center Passwords Changed HIPAA: Microsoft Operations Manager - Permissions Changed HIPAA: Microsoft Operations Manager - Windows Passwords Changed

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		HIPAA: Microsoft Sharepoint Permission Changed
164.312(c)(2)	Mechanism to Authenticate Electronic Protected Health Information (Addressable)	**Compliance Suite Alerts** (Cont.) HIPAA: RACF Passwords Changed HIPAA: RACF Permissions Changed HIPAA: TIBCO ActiveMatrix Administrator Permission Changed HIPAA: vCenter Orchestrator Login Failed HIPAA: vCenter Permission Change HIPAA: vCenter User Login Failed HIPAA: vCenter User Login Successful HIPAA: vCloud Director Login Failed HIPAA: vCloud Director Login Success HIPAA: vCloud User Created HIPAA: Windows Passwords Changed HIPAA: Windows Permissions Changed HIPAA: Pulse Connect Secure Successful Logins by IP

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.312(d)	Person or Entity Authentication (Required)	**Compliance Suite Reports** HIPAA: Account Activities on UNIX Servers HIPAA: Account Activities on Windows Servers HIPAA: Accounts Created on NetApp Filer HIPAA: Accounts Created on NetApp Filer Audit HIPAA: Accounts Created on Sidewinder HIPAA: Accounts Created on Symantec Endpoint Protection HIPAA: Accounts Created on TIBCO Administrator HIPAA: Accounts Created on TIBCO ActiveMatrix Administrator HIPAA: Accounts Created on UNIX Servers HIPAA: Accounts Created on Windows Servers HIPAA: Accounts Deleted on NetApp Filer HIPAA: Accounts Deleted on NetApp Filer Audit HIPAA: Accounts Deleted on Sidewinder HIPAA: Accounts Deleted on Symantec Endpoint Protection HIPAA: Accounts Deleted on TIBCO Administrator HIPAA: Accounts Deleted on TIBCO ActiveMatrix Administrator HIPAA: Accounts Deleted on UNIX Servers HIPAA: Accounts Deleted on Windows Servers HIPAA: Active Directory System Changes HIPAA: Cisco ISE, ACS Accounts Created HIPAA: Cisco ISE, ACS Accounts Removed HIPAA: Cisco ISE, ACS Password Changes HIPAA: ESX Accounts Activities HIPAA: ESX Accounts Created HIPAA: ESX Accounts Deleted HIPAA: ESX Group Activities HIPAA: F5 BIG-IP TMOS Password Changes HIPAA: Group Activities on NetApp Filer Audit HIPAA: Group Activities on Symantec Endpoint Protection

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.312(d)	Person or Entity Authentication (Required)	Compliance Suite Reports (Cont.) HIPAA: Group Activities on TIBCO ActiveMatrix Administrator HIPAA: Group Activities on UNIX Servers HIPAA: Group Activities on Windows Servers HIPAA: HP NonStop Audit Permissions Changed HIPAA: i5/OS DST Password Reset HIPAA: i5/OS Network User Profile Creation HIPAA: i5/OS Network User Profile Deletion HIPAA: i5/OS Object Permissions Modified HIPAA: i5/OS User Profile Creation HIPAA: LogLogic Management Center Account Activities HIPAA: LogLogic Management Center Password Changes HIPAA: Microsoft Operations Manager - Windows Accounts Activities HIPAA: Microsoft Operations Manager - Windows Accounts Created HIPAA: Microsoft Operations Manager - Windows Password Changes HIPAA: Microsoft Operations Manager - Windows Permissions Modified HIPAA: Microsoft Sharepoint Permissions Changed HIPAA: NetApp Filer Password Changes HIPAA: Password Changes on Windows Servers HIPAA: Permissions Modified on Windows Servers HIPAA: RACF Accounts Created HIPAA: RACF Accounts Deleted HIPAA: RACF Password Changed HIPAA: RACF Permissions Changed HIPAA: Symantec Endpoint Protection Password Changes HIPAA: TIBCO Administrator Password Changes HIPAA: TIBCO Administrator Permission Changes HIPAA: TIBCO ActiveMatrix Administrator Permission Changes

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
164.312(d)	Person or Entity Authentication (Required)	**Compliance Suite Reports** (Cont.) HIPAA: vCenter User Permission Change HIPAA: vCloud User Created HIPAA: vCloud User Deleted or Removed **Compliance Suite Alerts** HIPAA: Accounts Created HIPAA: Accounts Deleted HIPAA: Active Directory Changes HIPAA: Cisco ISE, ACS Passwords Changed HIPAA: Groups Created HIPAA: Group Members Added HIPAA: HP NonStop Audit Permission Changed HIPAA: i5/OS Permission or Policy Change HIPAA: IBM AIX Password Changed HIPAA: LogLogic Management Center Passwords Changed HIPAA: Microsoft Operations Manager - Permissions Changed HIPAA: Microsoft Operations Manager - Windows Passwords Changed HIPAA: Microsoft Sharepoint Permission Changed HIPAA: RACF Passwords Changed HIPAA: RACF Permissions Changed HIPAA: TIBCO ActiveMatrix Administrator Permission Changed HIPAA: vCenter Permission Change HIPAA: vCloud User Created HIPAA: Windows Passwords Changed HIPAA: Windows Permissions Changed