THINSCALE TECHNOLOGIES

THINKIOSK & SECURE REMOTE WORKER

HIPAA WHITE PAPER

ROSHAN BOLOOR | QSA, ISO 27001 LEAD AUDITOR / IMPLEMENTOR

COALFIRE

North America | Europe
877.224.8077 | info@coalfire.com | Coalfire.com

TABLE OF CONTENTS

EXECUTIVE SUMMARY

ThinScale Technology (ThinScale) commissioned Coalfire, a prominent cybersecurity risk management and compliance service provider, to perform an independent technical assessment of their ThinKiosk (ThinKiosk) & Secure Remote Worker (Secure Remote Worker) product. Coalfire's assessment included various technical testing, architectural assessment, and compliance validation activities.

This document outlines the features of ThinKiosk & Secure Remote Worker that may enable Covered Entities and Business Associates to implement appropriate safeguards in their environments to meet the requirements of the Health Insurance Portability and Accountability Act (HIPAA). Based on sample testing and evidence gathered during the assessment, Coalfire will describe these features that may assist Covered Entities and Business Associates in meeting HIPAA's Security requirements. The requirements that are not applicable are listed in Appendix A.

ABOUT THINKIOSK

ThinKiosk is a versatile software solution that can transform any Windows endpoint, be it a PC, laptop, or tablet, into a lean, centralized thin client. With its user-friendly interface, ThinKiosk gives users access to their Virtual Desktop Infrastructure (VDI) environments, local applications, and web applications, all while maintaining a secure and centrally managed environment. VDI is a virtualization technology that enables remote access to a desktop on a remote server. ThinKiosk makes it easy for users to enjoy the benefits of VDI without the need for additional hardware or complicated configurations.

ABOUT SECURE REMOTE WORKER

Secure Remote Worker (SRW) is a software-based solution designed for Windows devices outside the corporate network. This innovative tool enables non-corporate devices to function both as a personal device and as a secure thin client for corporate use, all while keeping the underlying Windows OS intact. With Secure Remote Worker, there is no need to make any changes or reconfigurations to the device, nor to reboot, dual boot, or rely on external USB devices.

Secure Remote Worker (SRW) is an innovative software solution that enables users to convert their personal devices into secure, trusted endpoints for remote working or bring-your-own-device (BYOD) scenarios. With SRW, users can connect to the corporate environment in a secure workspace that meets corporate IT standards and security policies.

ThinKiosk & Secure Remote Worker provide a comprehensive solution that locks down the Windows environment to ensure secure access to VDI environments, local applications, and web applications. The solution can be configured to combine remote VDI resources with local applications, while providing secure access to web-based resources through a secure browser. System administrators can customize settings for display resolutions, keyboard and mouse controls, and other Windows features as needed. This powerful tool ensures that users can work efficiently and securely, while meeting corporate IT standards and policies.

ThinKiosk & Secure Remote Worker have some key functionality in enabling personal & corporate devices to become HIPAA compliant including;

- Windows Patch Management
- Windows Firewall Control

- Windows Security Centre Detection
- USB Device Blocking
- Application Execution Prevention (AEP)
- Service Execution Prevention (SEP)
- Restricted access to key operating system components

For More detailed descriptions of these functionalities see the ThinScale website here.

AUDIENCE

This assessment white paper has three target audiences:

1. **Healthcare Providers and Internal Audit Community:** This audience may be evaluating either ThinKiosk or Secure Remote Worker to assess a healthcare organization or Business Associate environment for HIPAA compliance.
2. **Administrators and Other Compliance Professionals:** This audience may be evaluating ThinKiosk or Secure Remote Worker for use within their organization for compliance requirements for both HIPAA and other security standards.
3. **Healthcare and Business Associate Organizations:** This audience may be evaluating either ThinKiosk or Secure Remote Worker for deployment in their Electronic Protected Health Information (ePHI) data environment to simplify compliance with the HIPAA Security Rule

METHODOLOGY

Coalfire completed a multi-faceted technical assessment during the course of this project using the below industry and audit best practices. Coalfire conducted technical testing from March 1st, 2023, to March 27th 2023.

At a high level, testing consisted of the following tasks:

1. Technical review of the architecture of the full ThinKiosk and Secure Remote Worker solution and its components.
2. Implementation of the software in the Coalfire lab environment on the following OSs:
   a. Windows 10
3. The software runs in the following three modes, all of which were tested:
   a. ThinKiosk Shell - The desktop is completely empty except for the ThinKiosk panel
   b. Windows Shell - A full Windows desktop displayed, but with limited functionality
   c. Secure Remote Worker - Similar to the ThinKiosk Shell, with only the ThinKiosk panel on the desktop. This mode is the most common implementation.
4. During testing, access was attempted to the following Windows features, both by accessing the feature directly as it was intended to be used and by unconventional means that might be employed by a malicious user:
   a. Command Prompt
   b. Windows Explorer
   c. Control Panel
   d. Internet Settings

e. Remote Desktop

f. Task Manager

g. Ctrl+Alt+Del

h. Run command textbox in Start Menu

i. USB mass storage device access

j. Administrative Tools Services and Password Policies

k. User accounts

l. Windows Event Logs

m. Malware detection and anti-virus protection

n. Attempting to run an application configured to be blocked by the ThinKiosk & Secure Remote Worker Application Execution Prevention feature

o. Attempting to run a Windows service configured to be blocked by the ThinKiosk Service Execution Prevention and Windows Service/Device Driver Validation feature

5. A controlled sample of malware was installed on the Windows 10 test system to observe how ThinKiosk & Secure Remote Worker handled malware detection and protection. In addition, anti-virus software was turned off for one test to monitor how ThinKiosk & Secure Remote Worker managed anti-virus software and updates.

SUMMARY FINDINGS

The following findings are relevant highlights from this assessment:

- When properly implemented following vendor guidance, ThinKiosk & Secure Remote Worker provides coverage for the HIPAA controls listed in the Appendix A based on the sample testing and evidence gathered during this assessment.
- Either ThinKiosk or Secure Remote Worker can aid organizations in meeting specific requirements in both the Physical and Technical Safeguards of the HIPAA Security Rule.
- ThinKiosk & Secure Remote Worker was able to lockdown systems, as described in the documentation, preventing complete access to the following Windows features:
  - Command Prompt
  - Run command from the Start Menu
  - Ctrl+Alt+Del
  - USB mass storage device access
  - Addition of new users
  - Task Manager
  - Administrative Tools – Services and Password Policies
  - Application Execution Prevention successfully blocked an application that it was configured to block
  - Service Execution Prevention successfully blocked a Windows service that it was configured to block

- ThinKiosk & Secure Remote Worker were able to allow limited access to the following Windows features, but restricted the ability to change configurations to allow running software, other than ThinKiosk & Secure Remote Worker, on the test systems:
  - Control Panel
  - Internet Settings
  - Remote Desktop
  - Windows Explorer
- ThinKiosk and Secure Remote Worker offer the above-mentioned restrictions in all three modes of operation - ThinKiosk Shell, Windows Shell, and Secure Remote Worker. Additionally, the software generates comprehensive system logs that enable tracing of malicious activity, as required by HIPAA
- Either ThinKiosk or Secure Remote Worker adequately generated system logs of events such that malicious activity could be traced in accordance with the HIPAA specification Accountability (A) - §164.310(d)(2)(iii).
- Either ThinKiosk or Secure Remote Worker has an administrative password to prevent the software from being disabled by unauthorized users. The password can be setup by an administrator and made unique for each software installation, as required by the HIPAA specification Unique User Identification (R) - § 164.312(a)(2)(i) and Workstation Use - § 164.310(b). The software also logged user access, per the HIPAA specification Audit Controls - § 164.312(b).ThinKiosk and Secure Remote Worker can be tailored to the specific VDI requirements of the Windows system where they are installed. They also check for the status of anti-virus software, turn it on if necessary, and check for the latest Windows patches, security updates, and firewall status.
- Lastly, ThinKiosk and Secure Remote Worker provide Application Execution Prevention and Service Execution Prevention that can be configured to block designated applications and Windows services, enhancing system security.

ASSESSOR COMMENTS

The assessment focused on verifying the suitability of ThinKiosk and Secure Remote Worker in a healthcare setting, particularly with regards to complying with the HIPAA Security requirements. When implemented according to ThinScale Technology's guidance, these solutions can help Covered Entities and Business Associates meet all Physical and Technical Safeguards specified in the HIPAA Security Rule. While ThinKiosk and Secure Remote Worker can simplify HIPAA compliance by offering a comprehensive technical solution, it is important to note that each healthcare organization's computing environment is unique, and compliance is best achieved through a tailored combination of people, processes, and technology.

ThinKiosk and Secure Remote Worker are valuable tools that can enhance security controls for systems and networks. Healthcare organizations should prioritize security and business risk mitigation when selecting security controls.

It is worth noting that ThinScale Technology, through ThinKiosk and Secure Remote Worker, is not classified as a Covered Entity or Business Associate under HIPAA, as these solutions do not handle ePHI during creation, receipt, maintenance, or transmission.

TECHNICAL ASSESSMENT

ASSESSMENT METHODS

The assessment used the following methods to assess the potential safeguards of the ThinKiosk & Secure Remote Worker solutions aiding in HIPAA compliance:

1. Analysis of the architecture and configuration of the solution in accordance with vendor guidelines.
2. Deployment of ThinKiosk & Secure Remote Worker software to test machines along with enablement of strict policies to enforce lockdown of the Windows endpoints. Examination of the software configuration to confirm protection cannot be turned off by non-administrators.
3. Review of configurations and settings on each Windows test system while the software was deployed and running to verify all Windows features listed above were locked down.
4. Unlocking of the test systems using an administrative password to verify what had actually been inaccessible when the systems were locked down. The software was then turned on and the systems were locked down again to verify the same Windows features were once again inaccessible.

THINKIOSK & SECURE REMOTE WORKER COMPONENTS

ThinKiosk & Secure Remote Worker consists of the following components:

1. ThinKiosk & Secure Remote Worker Client – The client interface for software, which is installed on the PC. The GUI consists of a control panel that can be opened and displayed on the PC desktop or can be run minimized. When run as a non-administrative user, the GUI only provides access to the allowed Windows features and the VDI environment. When unlocked by an administrative user, the GUI allows full access to all previously blocked Windows functionality. The client also runs as a background process with the user interface minimized with a notification tray-based icon.
2. ThinScale Management Server– The management server is an optional component that can be installed on a backend server in the healthcare provider network. It can be used to manage multiple devices hosting ThinKiosk & Secure Remote Worker. ThinKiosk & Secure Remote Worker can be configured upon installation to use a local profile on the device where it is installed or to connect to and use a profile on the management server. When the management server is not deployed, ThinKiosk & Secure Remote Worker functions as a fully-featured standalone client. The management server is a web-based platform secured by HTTP/S.

ASSESSMENT ENVIRONMENT

ThinKiosk & Secure Remote Worker were installed in Coalfire's lab workstation Windows 10. The network environment was segmented from the Coalfire corporate network and the internet by a Cisco ASA 5525x stateful firewall.

Endpoint Diagram

Below is the typical endpoint architecture deployed within a healthcare provider environment.

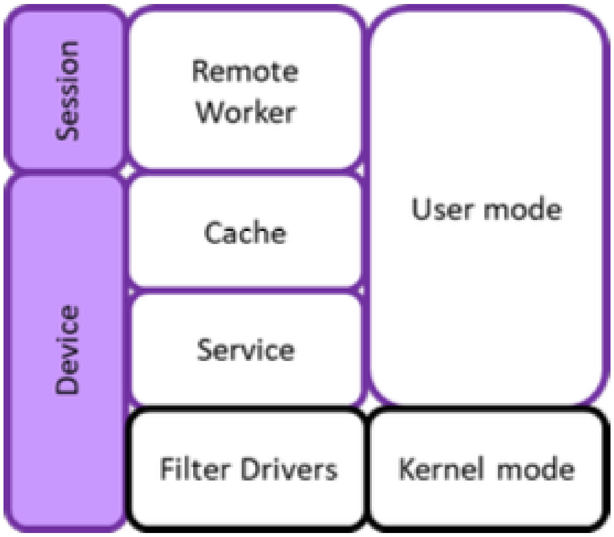

Figure 1: Endpoing Diagram

TOOLS AND TECHNIQUES

Standard tools Coalfire utilized for this application security review include:

TOOL NAME	DESCRIPTION
Windows Administrative Tools	The suite of native tools included with Windows were used to test ThinKiosk & Secure Remote Worker and verify that it locked down the PCs where it was installed. The following tools were used, or attempted to access: • Control Panel • Ctrl+Alt+Del • Services Panel of Administrative Tools • Password Policies panel of Administrative Tools • Windows Explorer • Task Manager • Windows Event Logs • User Accounts • Run Command Textbox in Start Menu • Internet Settings • Remote Desktop • Command Prompt

**Forensic tool: A tool or method for uncovering, analyzing, and presenting forensic data, which provides robust ways to authenticate, search, and recover computer evidence rapidly and thoroughly.*

REFERENCES

ThinScale website - https://thinscale.com/

Documentation provided by ThinScale:

- ThinScale_Architecture_Guide_7_x

HIPAA Compliance – https://www.hhs.gov/hipaa/for-professionals/index.html

APPENDIX A: HIPAA CONTROLS COVERAGE MATRIX

HIPAA Controls

Unlike other security standards, HIPAA does not specify particular technology solutions. So, for example, when HIPAA requires encryption, it simply states that encryption of ePHI is Addressable, rather than Required. It does not specify types of algorithms, minimum key lengths, or details of key management that are required for compliance, which might be detailed, or prescribed, in other standards. In HIPAA terminology, Addressable means that a HIPAA specification can be implemented exactly as stated in the standard without modification, or the specification can be implemented through a workaround that meets compliance. Addressable also allows a healthcare organization to not implement the specification, if it can show, and document, that implementation would not be reasonable in their environment. On the other hand, the term Required means, as the name implies, that the specification is required and must be implemented as specified. There are no workarounds allowed, or ways to opt out, as there would be for an Addressable specification.

The HIPAA Security Rule consists of the following three parts: Administrative, Physical, and Technical Safeguards. The Administrative and Technical Safeguards relate to the policies, procedures, and administrative requirements of the Rule, whereas the Physical Safeguards relate to how ePHI is physically protected. Related to the implementation of a solution such as either ThinKiosk or Secure Remote Worker, all of these Safeguards and their underlying requirements must be satisfied by the implementing organization to meet HIPAA compliance. However, ThinKiosk & Secure Remote Worker does support compliance with several of the HIPAA Security Rule requirements that fall under Technical Safeguards. These requirements, and their associated ThinKiosk & Secure Remote Worker controls, are detailed in the following table:

Key:

Compliance directly supported via use of ThinKiosk & Secure Remote Worker	🟢
Out of scope for ThinKiosk & Secure Remote Worker and requires healthcare provider action for full compliance	🟡

HIPAA CONTROLS	COMMENTS	COMPLIANCE SUPPORTED
164.312 (a)(1) **Access control – Implement technical policies and procedures for electronic information systems that maintain electronic protected health those persons or software programs that have been granted access rights as specified in 164.308(a)(4).**	The provision 164.312(a)(2)(1) of the HIPAA Security Rule requires healthcare organizations to implement policies and procedures to limit physical access to electronic information systems containing ePHI, and to allow access only to authorized individuals. ThinKiosk and Secure Remote Worker provide a reliable solution for controlling access to devices that can be used to create, receive, maintain, or transmit ePHI, helping organizations to meet this requirement. Furthermore, ThinKiosk and Secure Remote Worker offer an additional security feature called Application Execution Prevention (AEP), which enables the creation of a whitelist of approved applications that can be executed on the	🟡

HIPAA CONTROLS	COMMENTS	COMPLIANCE SUPPORTED
	system. This granular control is effective in preventing unauthorized applications or processes from running, thereby enhancing the security of ePHI. Additionally, AEP can be configured with targeted rule sets and digital signature checks to provide an extra layer of protection.	
164.312 (b) **Audit controls – Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that health information.**	ThinKiosk and Secure Remote Worker both have logs that monitor user access and events, allowing organizations to maintain user activity records for the device on which the program is installed. Additionally, the ThinKiosk Profile logging settings can be configured to suit specific needs. There is a feature that automatically saves changes made to the local virtual device, including files saved to the C: drive, to a temporary area that is deleted upon reboot. Moreover, both ThinKiosk and Secure Remote Worker have the Application Execution Control (AEP) feature, which allows organizations to whitelist applications to prevent unauthorized processes or applications from being executed. AEP can be configured down to the application level and can use targeted rule sets or digital signature checking.	✓
164.312 (c)(1) **Integrity – Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.** **164.312 (c)(1)(2) Implementation specification: Mechanism to authenticate electronic protected health information (Addressable). Implement electronic electronic protected health information has not been altered or destroyed in an unauthorized manner.**	164.312 (c)(1): Both ThinKiosk & Secure Remote Worker restrict access to crucial configuration settings by locking them down. This prevents users from changing daemons, services, and protocols from the desktop where the software is installed. The software also limits access to the Control Panel, the Run Command, Ctrl+Alt+Del, Task Manager, and the Services and Password Policies panels in Administrative Tools. This effectively blocks access to services that could be misused to alter or destroy ePHI. Additionally, the Service Execution Prevention feature can be used to block designated Windows Services and device drivers to prevent misuse. Both ThinKiosk & Secure Remote Worker can also block USB storage devices while still allowing essential devices, such as a keyboard and mouse, to function. 164.312 (c)(1)(2): The device running ThinKiosk or Secure Remote Worker can view ePHI data in a healthcare provider's ePHI data environment but cannot transmit or store the data. The ePHI data can only be accessed in read-only mode. To prevent the misuse of anti-virus software, ThinKiosk & Secure Remote Worker check for the presence and up-to-date status of anti-virus software on the device where it is installed. When the software starts up and locks down the device, it turns on the anti-virus software. If deployed, the ThinScale Management Server displays the status of anti-virus, anti-spyware, and firewall software. The software prevents users from continuing if the configured policy rules are not met, and remediation advice is provided.	✓
164.312 (d) Person or entity authentication – Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	It is the responsibility of healthcare providers to define unique access controls for each user as part of their processes. Both ThinKiosk and Secure Remote Worker	✓

HIPAA CONTROLS	COMMENTS	COMPLIANCE SUPPORTED
	software can assist organizations by providing technical authentication of individual users to the device.	
164.312(e)(1)Transmission security – Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	According to requirement 164.312 (e)(1), if the device is running ThinKiosk or Secure Remote Worker, it may have access to ePHI data. However, neither ThinKiosk nor Secure Remote Worker transmit this data back to the device or to their own software. Moreover, the ePHI data can only be viewed in read-only mode, ensuring that it remains unaltered.	🟡
Workstation Use **§164.310(b): Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.**	ThinKiosk & Secure Remote Worker both offer the ability to create and manage workstation and device profiles, including security configurations. This feature allows organizations to implement and monitor device settings in a streamlined and organized manner. Organization is responsible to implement policies and procedures that specify details governing access to ePHI	🟡
Device and Media Controls – Accountability **§164.310(d)(2)(iii): Maintain a record of the movements of hardware and electronic media and any person responsible therefore.**	If an organization utilizes the ThinScale Management Server in conjunction with either ThinKiosk or Secure Remote Worker, they may be able to establish and maintain accountability for their devices.	🟢
§164.308(a)(8) Evaluation **§164.308(a)(8): Perform a periodic technical and nontechnical evaluation based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, which establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.**	The logging and monitoring features provided by both ThinKiosk & Secure Remote Worker software can assist an organization in conducting a technical evaluation of its systems.	🟢

ABOUT THE AUTHOR

Roshan Boloor | Principal, **MBA, MS Cybersecurity, QSA, ISO/IEC 27001 Lead Auditor / Implementor**

Roshan Boloor is a Principal IT Security Consultant in the Payments Assurance practice at Coalfire for 10+ years. He advises senior management on how to meet their cybersecurity and IT governance, risk, and compliance (ITGRC) related goals. Roshan has assisted on multiple projects as a lead assessor for PCI DSS, HIPAA, HITRUST, ISO 27001, SOC2, and GDPR. Roshan has also provided support for clients as vCISO, vDPO, CSO, and HIPAA Officer. Roshan lead projects related to Information Technology General Controls (ITGC), IT risk assessments, vulnerability assessments, vendor risk management, social engineering, policy and procedure reviews. Roshan has worked extensively with cloud, software, telecommunication, service, retail, healthcare, financial institutions, and application providers. Roshan has worked closely with Coalfire tier-1 customers to help migrate to AWS, GCP, and Azure cloud environments.

Published April 2023.

ABOUT COALFIRE

Coalfire is the trusted cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for nearly 20 years and has offices throughout the United States and Europe. For more information, visit Coalfire.com.

Coalfire is solely responsible for the contents of this document as of the date of publication. The contents of this document are subject to change at any time based on revisions to the applicable regulations and standards (HIPAA, PCI-DSS et.al). Consequently, any forward-looking statements are not predictions and are subject to change without notice. While Coalfire has endeavored to ensure that the information contained in this document has been obtained from reliable sources, there may be regulatory, compliance, or other reasons that prevent us from doing so. Consequently, Coalfire is not responsible for any errors or omissions, or for the results obtained from the use of this information. Coalfire reserves the right to revise any or all of this document to reflect an accurate representation of the content relative to the current technology landscape. In order to maintain contextual accuracy of this document, all references to this document must explicitly reference the entirety of the document inclusive of the title and publication date; neither party will publish a press release referring to the other party or excerpting highlights from the document without prior written approval of the other party. If you have questions with regard to any legal or compliance matters referenced herein you should consult legal counsel, your security advisor and/or your relevant standard authority.