WHITE PAPER

THINKIOSK & SECURE REMOTE WORKER

HIPAA COMPLIANCE WHITE PAPER

ThinScale Technology

JOEL DUBIN | CISSP, QSA, PA-QSA

TERILYN FLOYD-CARNEY | CISSP, CISA, HCISSP, HITRUST CERTIFIED CSF PRACTITIONER, QSA, AND PA-QSA

COALFIRE

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

TABLE OF CONTENTS

EXECUTIVE SUMMARY

ThinScale Technology (ThinScale) engaged Coalfire, a leader in cybersecurity risk management and compliance services, to conduct an independent technical assessment of their ThinKiosk (ThinKiosk) & Secure Remote Worker (Secure Remote Worker) product. Coalfire conducted assessment activities including technical testing, architectural assessment, and compliance validation.

In this paper, Coalfire will describe the features of the software that might allow Covered Entities and Business Associates to incorporate safeguards into their environments to assist in their endeavors to meet the requirements of the Health Insurance Portability and Accountability Act (HIPAA). In this paper, Coalfire will describe, based on sample testing and evidence gathered during this assessment, the features of the software that might allow Covered Entities and Business Associates to incorporate safeguards into their environments to assist in their endeavors to meet the Security requirements of the Health Insurance Portability and Accountability Act (HIPAA). The requirements that were not applicable have been included in the matrix in Appendix A.

ABOUT BOTH THINKIOSK & SECURE REMOTE WORKER

both ThinKiosk & Secure Remote Worker is a software-only solution for any Windows endpoint, including PCs, laptops, and tablets, that converts the endpoint into a thin client. It creates a centrally managed and secure endpoint with a lightweight user interface that provides users access to their Virtual Desktop Infrastructure (VDI) environments. VDI is a virtualization technology that allows a user to remotely access a desktop on another server.

ABOUT SECURE REMOTE WORKER

Secure Remote Worker is a software-only solution for non-corporate Windows devices, that allows them to be used as a personal device as well as a secure corporate thin client all without the need to change or reconfigure the underlying Windows OS. It is achieved without the need to reboot, dual boot or use a USB device.

When enabled, SRW will convert users' personal devices into secure, trusted endpoints allowing them to be used for remote working or BYOD. SRW provides a secure workspace allowing them to connect to the corporate environment, all while ensuring corporate IT standards and security policies are met.

THINKIOSK OR SECURE REMOTE WORKER

Either ThinKiosk or Secure Remote Worker, depending on whether your endpoints are in-house or remote, locks down the Windows environment where it is installed, providing users with the access they need to log into their VDI environments, local applications and web applications. The solution can be configured to combine remote VDI resources with local applications while providing access to web-based resources through the secure browser. Other Windows settings, as needed, can be configured by system administrators for adjustment of display resolutions, keyboard, and mouse controls.

Both ThinKiosk & Secure Remote Worker have some key functionality in enabling personal & corporate devices to become PCI 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 either ThinKiosk or Secure Remote Worker for use within their organization for compliance requirements for 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 in their Colorado lab from September 18, 2017 to September 29, 2017, on February 13, 2018, and then again from December 20, 2018 to December 28, 2018.

Testing consisted of the following tasks:

1. Technical review was completed of the architecture of the full ThinKiosk & Secure Remote Worker solutions and its components.
2. Software was implemented in the Coalfire lab environment on the following OSs:
   - Windows 10
   - Windows 8.1
   - Windows 8
   - Windows 7
3. Software testing was conducted in all three modes of the application, as follows:
   - ThinKiosk Shell – The desktop is completely empty except for the ThinKiosk panel.
   - Windows Shell – A full Windows desktop is displayed, but with limited functionality.
   - Secure Remote Worker – Similar to the ThinKiosk Shell with only the ThinKiosk panel on the desktop. This mode is the most common implementation.
4. Access was attempted to the following Windows features, both normally as the feature was designed to be used and by unconventional means that might be employed by a malicious user:
   - Command Prompt
   - Windows Explorer
   - Control Panel
   - Internet Settings

- Remote Desktop
- Task Manager
- Ctrl+Alt+Del
- Run Command Textbox in Start Menu
- USB Mass Storage Device Access
- Administrative Tools – Services and Password Policies
- User Accounts
- Windows Event Logs
- Malware Detection and Anti-Virus Protection
- Attempting to run an application configured to be blocked by the ThinKiosk AEP feature
- Attempting to run a Windows service configured to be blocked by the ThinKiosk Service Execution Prevention feature

5. A controlled sample of malware was installed on the Windows 7 test system to check how ThinKiosk & Secure Remote Worker handled malware detection and protection. In addition, anti-virus software was turned off for one test to see 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, either ThinKiosk or Secure Remote Worker can provide a software-based thin client solution for endpoints on any Windows device.
- 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.
- Either ThinKiosk or Secure Remote Worker were 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
  - ThinKiosk AEP successfully blocked an application that it was configured to block
  - ThinKiosk Service Execution Prevention successfully blocked a Windows service that it was configured to block
- Either ThinKiosk or 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
- Either ThinKiosk or Secure Remote Worker provided the above restrictions in all three modes of the application.
- 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).
- Either ThinKiosk or Secure Remote Worker configurations can also be customized to the type of VDI required to be accessed from the Windows system, where it is installed.
- Either ThinKiosk or Secure Remote Worker checks to see if certain device settings have been disabled, such as firewalls, patch updates, and anti-virus. If the standard configurations have been changed, ThinKiosk can remotely return the settings to an enabled state.
- Either ThinKiosk or Secure Remote Worker AEP and Service Execution Prevention can be configured to successfully block designated applications and Windows services.

ASSESSOR COMMENTS

The assessment scope put a significant focus on validating the use of either ThinKiosk or Secure Remote Worker in a healthcare environment, specifically to include its impact on the HIPAA Security requirements. ThinKiosk or Secure Remote Worker, when properly implemented following guidance from ThinScale Technology, can be utilized by Covered Entities and Business Associates to meet all of the Physical and Technical Safeguards within the HIPAA Security Rule. The use of a solution such as either ThinKiosk or Secure Remote Worker may help streamline policies and procedures associated with HIPAA compliance by providing a multi-faceted technical solution. However, as most computing environments and configurations vary drastically, compliance with HIPAA is best accomplished using a customized combination of multiple elements of people, process, and technology.

ThinKiosk & Secure Remote Worker are tools that can be used to augment security best practice controls for systems and networks. Security and business risk mitigation should be any healthcare organization's goal and focus for selecting security controls.

Since ThinKiosk & Secure Remote Worker are not used in the creation, receipt, maintenance, or transmission of ePHI, ThinScale Technology, by way of ThinKiosk & Secure Remote Worker, is not a Covered Entity or Business Associate organization as defined by HIPAA.

TECHNICAL ASSESSMENT

ASSESSMENT METHODS

The following methods were used during this assessment to determine 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 either ThinKiosk or Secure Remote Worker software to test machines along with enablement of strict policies to enforce lockdown of the Windows endpoints.
3. Examination of the software configuration to confirm protection cannot be turned off by non-administrators.
4. 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.
5. Unlocking of the locked down test systems using an administrative password, and then locking them down again using the application, to verify that the application had actually blocked access to all Windows features listed above.

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 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 3.1 – The Management Server is an optional component that can be installed on a backend server in the healthcare network. It can be used to manage multiple devices hosting ThinKiosk or Secure Remote Worker. ThinKiosk or 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 function as a fully-featured standalone PC client. The Management Server is a web-based platform secured by HTTP/S.

ASSESSMENT ENVIRONMENT

ThinKiosk & Secure Remote Worker was installed in Coalfire's lab and implemented on four Virtual Machines running Windows 7, Windows 8, Windows 8.1, and Windows 10. Each system was running Windows Defender antivirus with auto-update enabled, which was turned on and off, as needed, during testing. The network environment was segmented from the Coalfire corporate network and the internet by a Cisco ASA 5525x stateful firewall.

TOOLS AND TECHNIQUES

Standard tools Coalfire utilized for this technical assessment review included:

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

REFERENCES

ThinScale Technology website - https://thinscale.com/

Documentation provided by ThinScale Technology:

- ThinKiosk Client Admin Guide
- ThinKiosk Profile Configuration Guide
- ThinScale Management Console 3.1.x Admin Guide
- ThinScale Management Server 3.1.x Admin Guide

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

APPENDIX A: HIPAA REQUIREMENTS COVERAGE MATRIX

HIPAA REQUIREMENTS

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 Physical 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:

Table Key:

Compliance directly supported via use of ThinKiosk & Secure Remote Worker = ✓

Part of Roadmap for features to be added in future releases of ThinKiosk & Secure Remote Worker = ✓

Out of scope for ThinKiosk & Secure Remote Worker and requires healthcare provider action for full compliance = ✓

HIPAA REQUIREMENT	COMMENTS	COMPLIANCE SUPPORTED
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 as specified in 164.308(a)(4).**	164.312 (a)(2)(1) Both ThinKiosk & Secure Remote Worker provides a tool for organizations to control access to devices that may be used to create, receive, maintain, or transmit ePHI. Both ThinKiosk & Secure Remote Worker also includes, through its AEP feature, whitelisting of applications that can be configured to prevent unauthorized processes or applications to be executed. AEP is granular down to the application level and can also be configured by targeted rule sets or checking if an application has a digital signature.	✓

HIPAA REQUIREMENT	COMMENTS	COMPLIANCE SUPPORTED
164.312 (b) **Audit controls – Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.**	Both ThinKiosk & Secure Remote Worker contains logs that monitor user access and events, allowing an organization to obtain and maintain user activity records for the device the program is installed on including logging settings set in the ThinKiosk Profile. The Roadmap for future releases includes adding a feature to automatically save changes to the local device, such as files saved to the C: drive, to a temporary area, which is deleted on reboot. Both ThinKiosk & Secure Remote Worker also includes, through its AEP feature, whitelisting of applications that can be configured to prevent unauthorized processes or applications to be executed. AEP is granular down to the application level and can also be configured by targeted rule sets, or checking if an application has a digital signature.	✓
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 mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.**	164.312 (c)(1) both ThinKiosk & Secure Remote Worker completely locks down access to any configurations for changing daemons, required services, and protocols from the desktop where the software is installed. The software limits access to the Control Panel, the Run Command in the Start Menu, Ctrl+Alt+Del, Task Manager, and the Services and Password Policies panels in Administrative Tools, effectively blocking access to services that could be misused to alter or destroy ePHI. In addition, the Service Execution Prevention feature added to both ThinKiosk & Secure Remote Worker can be configured to block designated Windows Services and device drivers to prevent misuse. Starting with version 5.2, both ThinKiosk & Secure Remote Worker can be configured to block USB storage devices, while still allowing essential devices using USB ports, such as a keyboard and mouse, to run. 164.312 (c)(1)(2) The device running either ThinKiosk or Secure Remote Worker may have access to view ePHI data in a healthcare provider's ePHI data environment, but that data is never transmitted back to the device or to ThinKiosk or Secure Remote Worker. The ePHI data would only be accessible to view in read-only mode. This requirement also covers implementation of anti-virus software, which could be used to alter or destroy ePHI. Both ThinKiosk & Secure Remote Worker currently checks if anti-virus software is either running or up-to-date on the device where it is installed. In	✓

HIPAA REQUIREMENT	COMMENTS	COMPLIANCE SUPPORTED
	addition, when the software starts up and locks down the device, it turns on the anti-virus software. Both ThinKiosk & Secure Remote Worker includes a feature that would detect if anti-virus, anti-spyware, and firewalls are installed and running. Their status would be displayed on the ThinScale Management Server 3.1 if deployed for either ThinKiosk or Secure Remote Worker. The software prevents the user from continuing if the configured policy rules are not met, for example, for anti-virus software, such as whether the anti-virus is running and up-to-date. Both ThinKiosk & Secure Remote Worker then displays remediation advice.	
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.**	Defining unique access controls for each user is a process-related requirement that would be the responsibility of the healthcare provider. Both ThinKiosk & Secure Remote Worker software could help an organization by providing technical authentication of an individual 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.**	164.312 (e)(1) The device running either ThinKiosk or Secure Remote Worker may have access to ePHI data, but that data is never transmitted back to the device or to either ThinKiosk or Secure Remote Worker. The ePHI data would only be accessible to view in read-only mode.	✓
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.**	Both ThinKiosk & Secure Remote Worker has the ability to define workstation and device profiles and security configurations, which may allow an organization to implement and track device settings.	✓
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.**	When the ThinScale Management Server 3.1 is utilized with either ThinKiosk or Secure Remote Worker, an organization may have the ability to maintain accountability for devices.	✓

HIPAA REQUIREMENT	COMMENTS	COMPLIANCE SUPPORTED
§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 capabilities of both the ThinKiosk & Secure Remote Worker software may aide an organization in the technical evaluation of the organization's systems,	✓

ABOUT THE AUTHORS

Joel Dubin | Senior Consultant

Joel Dubin (jdubin@coalfire.com) is a Senior Consultant and Application Security Specialist with Coalfire. Joel has several years of experience working as a QSA and PA-QSA helping clients develop systems and software for use in PCI DSS environments and has authored and spoken on multiple security topics including application security, cyber risk management, secure software development, and PCI DSS and PA-DSS compliance. He holds a CISSP, QSA, and PA-QSA.

QA:

Terilyn Floyd-Carney | Senior Consultant

Terilyn Floyd-Carney (tfloyd-carney@coalfire.com) is a Senior Consultant and Application Security Specialist with Coalfire. Terilyn has several years of experience working as a PA-QSA and HITRUST Certified CSF Practitioner helping clients develop systems and software for use in healthcare, pharmacy, and retail environments and has authored and spoken on multiple security topics including application security, cybersecurity best practices, and compliance. She holds a CISSP, CISA, HCISSP, HITRUST Certified CSF Practitioner, QSA, and PA-QSA.

Published February 2019.

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.