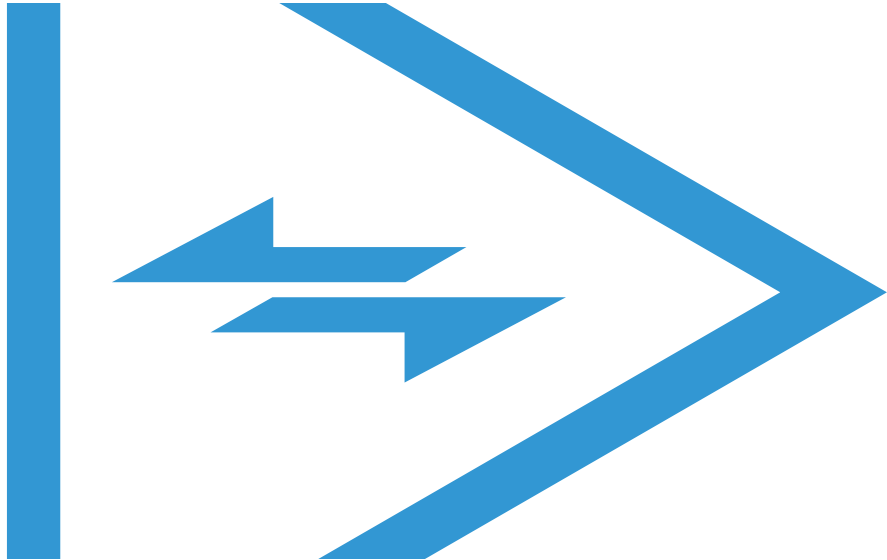


Service Categories:

VOICE & SPEECH RECOGNITION
WORKFLOW TECHNOLOGIES
OUTSOURCED SERVICES

MedQuistTM

PATIENT # ID: CODE:



CodeRunner and HIPAA

Health Insurance Portability and Accountability Act

Table of Contents

- 1 Introduction..... 3
- 2 CodeRunner MQ Overview..... 4
 - 2.1 Data Security 5
 - 2.1.1 Authentication 5
 - 2.1.2 Data Encryption..... 5
 - 2.1.3 Data Integrity 5
 - 2.2 Application Security..... 6
 - 2.2.1 System Access..... 6
 - 2.2.2 System Permissions and Restrictions..... 6
 - 2.2.3 Activity Auditing and Reporting..... 7
 - 2.3 System Security 8
 - 2.3.1 Physical Security 8
 - 2.3.2 Internet Security..... 8
- 3 CodeRunner and HIPAA 9
 - 3.1 HIPAA Final Rule for Security Standards..... 9
 - 3.2 How CodeRunner Supports HIPAA Requirements..... 9
 - 3.2.1 Administrative Safeguards..... 10
 - 3.2.2 Physical Safeguards..... 12
 - 3.2.3 Technical Safeguards..... 13
- 4 Conclusion 14

1 Introduction

The Health Insurance Portability and Accountability Act (HIPAA) was signed into law on August 21, 1996, its primary purpose to protect health insurance coverage for workers as their employment status changes. To that end, HIPAA includes an Administrative Simplification section intended to outline standards for the efficient and secure transfer of patient and health information, thereby reducing the administrative burden and associated costs involved in the sharing of such information between organizations.

At its foundation, the Administrative Simplification section establishes standards for the electronic transmission of many administrative, financial and healthcare transactions currently carried out on paper. These standards include:

- > Privacy Standards for Health Information
- > Security Standards for Electronic Health Information
- > Transactions and Code Sets

Healthcare providers, health plans and clearinghouses **must** comply with **all** of the prescribed standards. Health plans, clearinghouses and **providers must comply with the Security Standard if they handle individual health information in electronic form**. Providers must comply with the transaction and code sets only if they choose to use electronic means to perform the financial, administrative and healthcare transactions as defined in HIPAA.

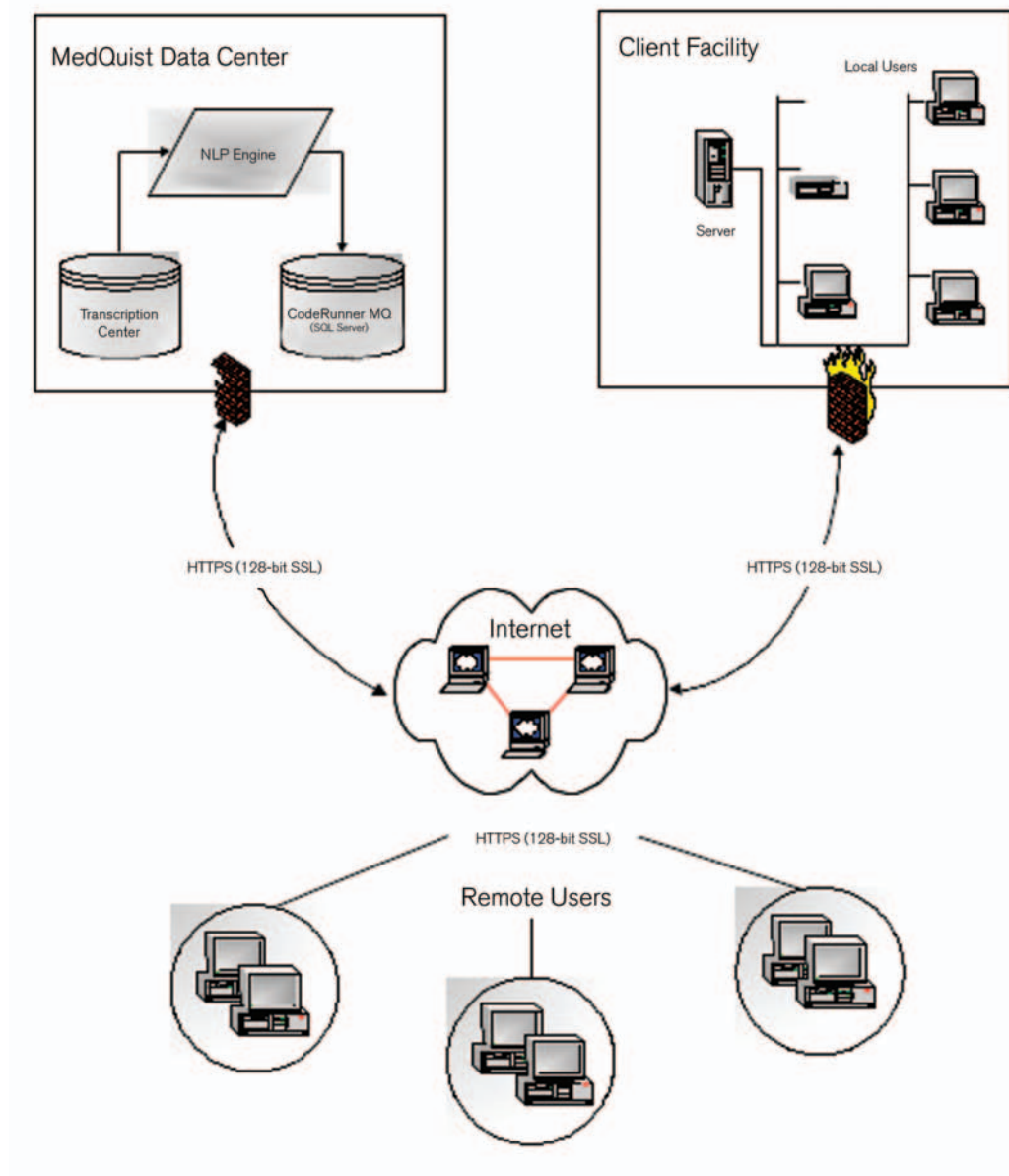
Given the significant importance and broad applicability of HIPAA's final security and privacy standards, the balance of this paper will discuss how MedQuist's CodeRunner technology and professional services can provide healthcare organizations with a secure, scalable remote coding solution particularly well suited to support the **security and privacy** requirements being imposed by HIPAA.

HIPAA covers an extremely broad range of issues from policy to technology. This paper is not intended to provide an all-inclusive discussion of HIPAA. Nor does this paper provide a detailed listing of CodeRunner features and capabilities. Rather, this paper provides an overview of the CodeRunner system, CodeRunner approach to security and a brief analysis of how CodeRunner supports an organization's efforts to comply with HIPAA's security and privacy standards.

2 CodeRunner MQ Overview

MedQuist's CodeRunner is a web-enabled, thin-client medical record coding and workflow system deployed as an Application Service Provider (ASP) centrally hosted and accessible via the Internet. Built using sophisticated application security techniques and state-of-the-art technologies from Microsoft, MedQuist's CodeRunner provides healthcare organizations with a scalable, secure technology solution.

Figure 1: CodeRunner Context Diagram



The sections that follow provide a brief discussion of the CodeRunner security and data privacy capabilities and architecture. Specifically, MedQuist offers three layers of data security with its CodeRunner application offering.

- > Data Security
- > Application Security
- > System Security¹ (including physical security of the MedQuist Data Center)

2.1 Data Security

The CodeRunner data security approach provides capabilities for user authentication, data encryption and data integrity. As a fully web-enabled, thin-client application, CodeRunner utilizes Hyper Text Transfer Protocol (HTTP) to support communications between the client application and the back-end CodeRunner application servers, and therefore takes advantage of the secure option to HTTP – HTTPS. HTTPS is the publicly accepted standard for protecting Internet-based HTTP communications and employs Secure Sockets Layer (SSL) to secure the HTTP communications. SSL-enabled HTTP provides multiple levels of data security, including authentication, data encryption and data integrity. Each level of data security is described in more detail below.

2.1.1 Authentication

SSL authentication allows clients to validate a server's identity through the use of digital certificates. Digital certificates are the digital equivalent of one's legal signature. Digital certificates uniquely identify an entity, whether it's a web server or an individual. SSL uses standard public-key cryptography techniques to validate the server's digital certificate. This ensures that the HTTP communications occur only with authorized servers, thereby protecting data from being read, understood and/or used by anyone else on the network (i.e., Internet or private network).

In short, the use of SSL authentication means CodeRunner users can be sure they are communicating with the CodeRunner servers and only CodeRunner servers.

2.1.2 Data Encryption

Data encryption ensures the privacy of data while being transmitted via the Internet. CodeRunner uses 128-bit HTTPS to encrypt all information exchanged between the CodeRunner client application and CodeRunner servers. HTTPS encryption, at the 128-bit level, is publicly regarded as acceptable for all sensitive healthcare and medical record information.

2.1.3 Data Integrity

Data integrity is the ability to protect data from being changed or tampered with. All data sent over an encrypted HTTPS connection is protected with a cryptographic mechanism for detecting tampering – that is, for automatically determining whether the data has been altered while in transit.

¹ In the context of this document, "physical security" only refers to the facilities over which MedQuist has positive control (i.e., MedQuist's data centers).

2.2 Application Security

Application security represents the layer of security through which the application controls:

- > system access,
- > system privileges and restrictions, and
- > activity auditing and reporting.

The CodeRunner application is built upon a layered application security architecture that uses a combination of unique user identifiers and passwords, role-based permissions, system access privileges and system auditing.

2.2.1 System Access

CodeRunner controls system access in two important ways. First, all users must present a valid user ID and password to gain access to the CodeRunner application, regardless of the functionality being accessed. Second, CodeRunner sessions are automatically terminated to protect against unauthorized access from a logged on computer that has been left unattended.

User ID and Passwords

While an individual's user ID is not generally considered confidential², an individual's password must remain secret, only known by its owner. Therefore, to better ensure password confidentiality, CodeRunner stores and maintains user passwords in an encrypted form known as a digital message digest or hash³. As a result, the only way to validate a submitted clear-text password is to hash the password and compare it to the stored hash value. Since clear-text passwords are submitted via HTTPS, thereby encrypted during transit and never stored or compared, maximum password security is provided. In addition, password expiration dates can be configured through CodeRunner system administration.

Session Timeout (Auto-logout)

CodeRunner automatically monitors every active session to protect against unauthorized access from a logged on computer that has been left unattended. Sessions with inactivity for a specified period are ended and the user for that session is automatically logged off the system, with an appropriate entry to the activity audit log. While the system default is 20 minutes, the timeout period can be set in one-minute increments.

2.2.2 System Permissions and Restrictions

CodeRunner controls system permissions and restrictions through an innovative implementation of a traditional role-based security model. The CodeRunner application establishes **“roles”** as a basis for defining “need to know” access to information and permissions consistent with a user's job duties. System function privileges, which are grantable permissions within the system, are then assigned to roles providing a baseline set of permissions for a given role. Users are then assigned to defined roles based on their job duties, and subsequently, inherit the permissions granted to the roles to which they are assigned.

Because CodeRunner has been designed to support deployment as a true Application Service Provider (ASP) offering, and therefore must support multiple clients concurrently, the role-based model implemented in CodeRunner has benefited from further refinement.

² In fact, user IDs are often components of an individual's e-mail address.

³ A hash is a one-way encryption using the SHA1 algorithm, meaning there is no known decryption method for the hashed data.

2.2.2 System Permissions and Restrictions, *continued*

More specifically, the CodeRunner role-based security model has been extended to include the additional concept of **“groups.”** Groups are created and managed at the client level and allow MedQuist and its clients the ability to provide a more granular distinction between similar but different groups of users. Groups are created and must be assigned to one of the system-defined roles. As a result, system permissions and restrictions can be granted at the Group, Role and User level, providing maximum flexibility and security.

All system privileges and restrictions are managed through the CodeRunner System Administration (SA) module. Access to the SA module is limited to authenticated users previously granted the system administrator privileges.

2.2.3 Activity Auditing and Reporting

While access control is important, CodeRunner also tracks and logs user activity to further ensure that those who do have valid access to the system do not jeopardize the integrity of the system through inappropriate actions. CodeRunner accomplishes this through a combination of activity auditing, data and document versioning and detailed reporting.

CodeRunner audits and logs sensitive system activity such as the following:

- > User access – log on and off activity
- > Session timeouts (auto-logoffs)
- > Patient record access
- > Encounter code modifications
- > Document viewing and editing

In addition to activity auditing and logging, CodeRunner provides versioning of all patient and medical record data modified within the system. Versioning includes a history record of all “before” and “after” changes, when the changes were made, who made the changes and why. This allows for a complete audit trail of all modifications to patient and medical record data.

Lastly, CodeRunner provides a comprehensive set of reports designed to provide insight into the audited activities and version control information.

2.3 System Security

MedQuist hosts the CodeRunner ASP at the SunGard Data Center in Alpharetta, Georgia.

SunGard: SunGard (NYSE:SDS) is a global leader in integrated IT solutions and eProcessing for financial services. SunGard is also the pioneer and a leading provider of high-availability infrastructure for business continuity. With annual revenues in excess of \$1 billion, SunGard serves more than 20,000 clients in over 50 countries, including 47 of the world's 50 largest financial services institutions.

MedQuist's ability to provide the appropriate level of system security is critical to guarantee the safety and security of patient medical information. The data center is secured at both the physical and Internet levels.

2.3.1 Physical Security

MedQuist's data center is hosted in a leading "co-location" facility, located in Atlanta. This facility provides the physical environment necessary to ensure the CodeRunner system remains operational and available 24 hours a day, 7 days a week.

In addition to raised floors and a sophisticated HVAC temperature control systems with separate cooling zones, the MedQuist data center offers a wide range of physical security features including state-of-the-art smoke detection and fire suppression systems, 24x7 secured access, key card and Biometric access to secured areas and video camera surveillance and security breach alarms. Furthermore, access doors are always monitored and alarmed for tamper protection.

When visiting the data center, visitors are required to sign in at the security desk. Initial entry to the building is controlled by an access card. The combination of access card and fingerprint identification further controls access to the hosting center. In addition to the electronics described, an impenetrable wire mesh running from under the raised flooring to the top of the ceiling further guarantees protection from intrusion. Lastly, there is never visual access to any computer equipment from outside the data center-controlled area.

2.3.2 Internet Security

Nokia IP440 is the hardware; the firewalling application is called Checkpoint Firewall 1. It is the leading brand and provides "stateful inspection" of the data being transmitted; this has become the de facto standard for firewall technology.

3 CodeRunner and HIPAA

As the CodeRunner product primarily targets healthcare providers, this section serves to summarize the requirements surrounding the Security Rule and highlight how various CodeRunner features implement capabilities necessary to meet the Security Rule requirements.

3.1 HIPPA Proposed Rule for Security Standards

The Final Security Rule identifies basic standards on how to protect the integrity, confidentiality and availability of electronic health information. The standard is divided into the following three areas: administrative, physical and technical safeguards.

- > Administrative safeguards address the planning, policies and personnel regarding how to implement the standards and manage the conduct of the workforce.
- > Physical safeguards address the physical measures to protect electronic health information and its information systems, equipment and buildings against environmental and natural hazards and unauthorized intrusion.
- > Technical safeguards address what technical features need to be enabled on applications and products to protect electronic health information and to control access to it.

3.2 How CodeRunner Supports HIPPA Requirements

The tables that follow are organized by the three areas listed above, and they enumerate HIPAA requirements, their corresponding implementations specifications and applicable MedQuist technologies, policies and procedures.

There are several HIPAA requirements that do not apply to MedQuist's CodeRunner offering. Such requirements are not listed in the tables that follow.

Please note that the organization and HIPAA-specific content of the tables were taken from ***Department of Health and Human Services Security Standards; Final Rule***, dated February 20, 2003.

3.2.1 Administrative Safeguards

Administrative safeguards address the planning, policies and personnel of how to implement the standards and manage the conduct of the workforce.

HIPAA Requirement	Implementation Specifications	Applicable CodeRunner Features
Contingency plan	<ul style="list-style-type: none"> > Data backup plan > Disaster recovery plan > Emergency mode operation plan > Testing and revision 	MedQuist Standard Operating Procedures include system-testing, data backup, disaster recovery and emergency mode plans.
Information access management	<ul style="list-style-type: none"> > Access authorization > Access establishment > Access modification 	<p>MedQuist offers three layers of security:</p> <ul style="list-style-type: none"> > Physical Security (physical security of the data center); > Data Security (CodeRunner data encryption); and > Application Security (user authentication, complete with user, role and group-based access control).
Workforce security	<ul style="list-style-type: none"> > Supervision of maintenance personnel > Workforce clearance procedure > Termination procedures 	<p>The MedQuist Data Center is managed and operated by a team of highly trained technology professionals, operating in accordance with established standard operating procedures.</p> <p>CodeRunner security features support termination procedures:</p> <ul style="list-style-type: none"> > Removal from access lists > Removal of user account(s)
Security incident procedures	<ul style="list-style-type: none"> > Report procedures > Response procedures 	<p>MedQuist Data Center Standard Operating Procedures address security incident reporting and response.</p> <p>In addition, MedQuist works closely with clients during implementation to integrate client reporting and response procedures with those of the data center.</p>

3.2.1 Administrative Safeguards *continued*

HIPAA Requirement	Implementation Specifications	Applicable CodeRunner Features
Security management process	<ul style="list-style-type: none"> > Risk analysis > Risk management > Sanction policy > Information system activity review 	<p>The MedQuist Data Center's Standard Operating Procedures address risk analysis and management. In addition, MedQuist Workforce Sanctions Policy addresses sanction procedures for our workforce.</p> <p>In addition, CodeRunner includes a sophisticated activity auditing capability that tracks and reports user activities within the system.</p>
Security awareness and training	<ul style="list-style-type: none"> > Awareness training for all personnel (including management) > User education concerning virus protection > The importance of monitoring login success/failure, discrepancies > User education in password management 	<p>MedQuist has a documented training plan that includes comprehensive employee orientation and security and privacy training.</p>

3.2.2 Physical Safeguards

Physical safeguards address the physical measures to protect information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.

HIPAA Requirement	Implementation Specifications	Applicable CodeRunner Features
Media controls	<ul style="list-style-type: none"> > Accountability (tracking mechanism) > Data backup and storage > Media re-use > Disposal 	<p>The procedures regarding data backup, storage and disposal, including the receipt and removal of backup tapes, are included in the Data Center's Standard Operating Procedures.</p>
Facility access controls	<ul style="list-style-type: none"> > Contingency operations > Access control and validation procedures > Facility security plan > Maintenance records 	<p>The MedQuist Data Center limits unauthorized access to computer systems, displays and networks. The facility is equipped with state-of-the-art smoke detection and fire suppression systems, and 24x7 secured access, including key card and Biometric access to secured areas, as well as video camera surveillance and security breach alarms.</p> <p>In addition, CodeRunner includes a sophisticated activity auditing capability that tracks and reports user activities within the system.</p>
Workstation use	None	<p>The MedQuist Data Center limits unauthorized access to computer systems, displays and networks. The facility is equipped with state-of-the-art electronic access control and surveillance systems deployed to control and track access to the facility.</p> <p>MedQuist has a documented training plan that includes a comprehensive employee orientation and security and privacy training program.</p>
Workstation security		

3.2.3 Technical Safeguards

Technical safeguards address the security features that need to be enabled on applications, products and information systems to protect electronic-specification protected health information and control access to it.

HIPAA Requirement	Implementation	Applicable CodeRunner Features
Access control	<ul style="list-style-type: none"> > Unique user identification > Procedure for emergency access > Automatic log off > Encryption and decryption 	<p>The CodeRunner application requires user and password authentication.</p> <p>In addition to traditional user authentication, the CodeRunner application controls access to information and functionality based on any one or a combination of these: user, role and group.</p>
Audit controls		<p>The CodeRunner application provides exhaustive activity auditing and logging, capturing data versions, time, session, workstation, event and user information. The CodeRunner application audits every event in the system, capturing date, time, session, workstation, event, version, old data, new data and user information.</p>
Integrity	None	<p>The CodeRunner application leverages SSL's check sum processing to ensure the integrity of transmitted data.</p>
Person or entity authentication	None	<p>The CodeRunner application has configurable parameters on user and person authentication.</p>
Transmission security	<ul style="list-style-type: none"> > Integrity controls > Encryption 	<p>The CodeRunner application leverages SSL's check sum processing to ensure the integrity of transmitted data.</p> <p>Lastly, the CodeRunner application is fully web-enabled and completely compatible with 128-bit encryption used with secure sockets layer communications (SSL).</p>

4 Conclusion

MedQuist has been able to leverage its economics of scale to provide a state-of-the-art solution that combines advanced application features and state-of-the-art software and hardware to provide the unparalleled security for a computer-assisted, remote coding solution.

FOR MORE MEDQUIST WHITE PAPERS, VISIT US ONLINE AT MEDQUIST.COM OR CALL 1.866.534.9004