



Stoneware™ webNetwork

Helping HIPAA Compliance

Stoneware, Inc.

Published: October 2008

This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein. The information contained in this document represents the current view of Stoneware, Inc. on the issues discussed as of the date of publication. Because Stoneware must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Stoneware, and Stoneware cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Stoneware, Inc. MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Stoneware, Inc..

Stoneware may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Stoneware, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2007 Stoneware, Inc. All rights reserved.

The names of actual companies and products mentioned herein may be the trademarks of their respective owner

Introduction

Stoneware's webNetwork is a "Universal Web Access" connector presenting applications and information in either a webOS or portal interface. Healthcare organizations can leverage webNetwork's advanced technology to *assist* in meeting their HIPAA (Health Insurance Portability and Accountability Act) compliance requirements while delivering secure remote access, Intranet, and Extranet solutions to their growing mobile physician and patient network.

This document will overview some of the key webNetwork technologies and how they can *assist* in meeting the specific categories defined within the HIPAA Security Standards Matrix. Again,

Workforce Security - 164.308(a)(3)

Stoneware's complete integration with an organization's directory service will assist in the meeting the addressable concerns in workforce security.

- Authorization and / or Supervision – webNetwork allows organizations to control access to webNetwork and integrated systems either by the user's identity or their physical network IP address/subnet.
- Workforce Clearance Procedure – webNetwork leverages directory services assignment already defined by the healthcare organization to control access to healthcare applications, data, and services.
- Termination Procedure – because webNetwork utilizes an organization's network directory service as the authentication source, disabling network access to a terminated employee will automatically remove access to all applications and services available through webNetwork.

Information Access Management – 164.308(a)(4)

Stoneware's webNetwork flexible management architecture and directory service integration assists healthcare organizations in the implementation of their access control policies and procedures.

- Access Establishment and Modification – webNetwork's Role-based Access Control model allows healthcare organizations to control access to applications, databases, data records, and services at a user, group, or organizational level.

Security Awareness and Training 164.308(a)(5)

webNetwork assists healthcare organizations with their security awareness and training by providing login monitoring and password management services.

- Login Monitoring – webNetwork allows organizations to monitor the logged in users that authenticate to the system. webNetwork will track the current logged in users, their login time, activity, and last known activity.
- Password Management – webNetwork provides several features that can be utilized in the management of passwords for both the webNetwork system and the applications and services accessed through the system.
 - Lockbox – encrypts and secures credentials to systems that are accessed via webNetwork. Secures access to credentials by the user's directory service identity. Encrypts credentials using a unique key and encryption method known as "blowfish".
 - Lockbox Masks – allows administrator to configure password masks that will match the application's password restrictions. Masks can force the end user to meet certain password restrictions such as length, numeric, special characters, etc before updating the lockbox.
 - Password Configuration – webNetwork provides the facilities for setting, changing, and resetting user passwords either by the administrators of the system or the end users. These facilities can be utilized by the healthcare organization as part of their password management procedures.

Security Incident Procedures 164.308(a)(6)

webNetwork provides system logging and reporting features that will assist healthcare organizations in reporting and monitoring incidents as they pertain to data and application access. The logging engine within webNetwork will log all authenticated and non-authenticated requests either to a standard web log or to a common JDBC / ODBC database. The reporting engine embedded within the webNetwork product will allow administrators to create reports that can detail and summarize user access to both applications and services protected by the webNetwork system. These reports can be distributed to security, HIPAA, and management personnel through the portal interface or by email.

Contingency Plan 164.308(a)(7)

webNetwork can assist in the delivery of critical electronic applications and services that are a part of any healthcare organization's disaster recovery and business continuity plan.

- Emergency Mode Operation Plan – webNetwork can provide remote and displaced users with secure remote access to critical healthcare systems and data during a disaster. webNetwork can be setup in a "session-level" clustered configuration that will automatically detect a system failure and

initiate a fail-over to an off-site facility.

- Testing and Revision Procedure – webNetwork can play a role in the organization’s disaster recovery testing procedures. webNetwork’s automatic fail-over and fault tolerance allows organizations to test the fail-over of an individual application or service to an off-site location or the complete system.
- Applications and Data Criticality Analysis – webNetwork can be configured to reflect the healthcare organization’s business continuity plan. Based on the organization’s assessment of specific applications and data, webNetwork can be configured to fail-over specific applications and databases that have been deemed critical to the operations of the business.

Workstation Security 164.310(c)

webNetwork can assist in organization’s in restricting access to specific machines based on either the assignment of an IP address or the presence of a USB device on the physical workstation.

- IP Address – webNetwork will control access to healthcare applications and services based on the IP address or the IP subnet configured on the local workstation.
- USB Key – webNetwork can control the access of an end user based on the presence of a uniquely identified USB device on the physical workstation. The USB device can be assigned to an individual user, group of users, or an entire organization.

Access Control 164.312(a)(1)

webNetwork leverages an organization’s network directory service to define and identify a user’s unique digital identity. It is their identity that drives all authentication, access control, and configuration of services and applications.

- Unique User Identification – a user’s identity is defined by their unique network ID. In addition, the webNetwork system can leverage other directory attributes on a user’s identity such as email address, PIN, employee number, etc to control access to record-level information in most databases.
- Emergency Access Procedure – because webNetwork leverages a replicatable directory store for all authentication and access control information, healthcare organizations can define a redundant off-site directory agent which can be utilized by webNetwork during a disaster to maintain consistent access control and authentication procedures.

- Automatic Log-off – the webNetwork Server has an embedded inactivity timer that can be configured to match the organization’s policy on inactive users. The inactivity timer will automatically terminate a user’s session based on the amount of time the user has been inactive within the system.
- Encryption / Decryption – the webNetwork Relay, which acts as the secure entry point into the webNetwork system, is responsible for all encryption and decryption of data and applications during wire transmissions between the system and user. Users that are requesting access to applications and data via the webNetwork system will have all communications encrypted in 128bit SSL (Secure Socket Layer) communications.

Audit Controls 164.312(b)

webNetwork can assist in the auditing of access to healthcare applications and data by tracking all requests made by both authenticated and non-authenticated users through the webNetwork system. The data collected is written to a standard web log or a backend JDBC/ODBC database based on configuration. Both administrators and management personnel can build custom reports for examining access to applications and services within the system.

Person or Entity Authentication 164.312(d)

webNetwork can assist healthcare organizations in validating the integrity of users accessing applications and data by leveraging its two-factor authentication features. Two factor authentication forces the end user to validate their identity by another factor before allowing access to critical information and applications. webNetwork supports the following two-factor authentication methods:

- Biopassword – two-factor biometric authentication system which matches a user’s credentials with their unique typing rhythm. Biopassword will use keyboard heuristics as the second factor of authenticate to validate the user’s true identity.
- Tokens – two-factor authentication system matching a user’s credentials with a physical security token to validate the user’s identity. Token vendors include SecurID and ActivIdentity.
- USB Keys –two-factor authentication system matching a user’s credentials with a physical USB key to validate the user’s identity. webNetwork supports most standard USB keys from a large number of vendors.
- Directory Attributes – two-factor authentication method that utilizes a second identity attribute (i.e. – PIN, workforce ID, email, etc) to validate the user’s identity.

Transmission Security 164.312(e)(1)

webNetwork can assist in the encryption of electronically transmitted healthcare information by providing several points at which the communications and/or the data is encrypted.

- Encryption - encrypted transmission between the user and system – the webNetwork Relay is capable of encrypting all transmissions between the end user and the webNetwork system with SSL (Secure Socket Layer).
- Integrity Controls – webNetwork’s reporting engine can be utilized by a healthcare organization as an alternative to giving end users application access. The benefits of reporting, versus delivering a complete application, is the capability of the organization to restrict the user’s rights to the information. Report services can be utilized to securely distribute and display healthcare information that has been generated from a backend database. Reports can be configured (based on identity) to display information that can only be viewed by the end user and never modified.

* This document is intended to help healthcare organizations in better understanding how Stoneware’s webNetwork in assist complying to HIPAA laws and regulations. This document is not intended to act as a guide or imply that implementing webNetwork will, by itself, meet the requirements needed for HIPAA compliance.