MD Coder Software Security Overview

Revision History

Version	Change	Author	Date
1.1	Initial Revision	D.S	2/7/2008
1.2	Update Revision	F.R.	11/13/2008
1.3	Update Revision	D.S.	1/20/2011
1.3	Update Revision	F.R.	7/15/2012
1.3	Update Revision	F.R.	4/2/2013
1.3	Update Revision	F.R	1/20/2014

This document describes the security architecture of the MD Coder software solution including all mobile clients. It also includes a list of common security related questions in a Q&A format to assist with the decision making process.

Security Overview

Overview

MD Coder is a charge capture solution for physicians which allows users to efficiently and accurately capture patient demographic, encounter and charge information at the point of care.

The MD Coder solution is a suite of software comprised of a web application ("MD Coder Web Edition") and mobile clients. The platforms currently supported by a mobile client are:

- Blackberry (touch and non-touch versions)
- iPhone
- iPad
- Android

Authentication and Authorization

The device requires an active user account comprised of a user name and associated password. The device can also optionally be required to ask for PIN in order to access information on the device. The application can be integrated with a directory using LDAP and has the ability to specify and enforce password length rules. The system utilizes role based authentication and logs both attempted and successful logins for audit purposes. Passwords are not stored.

Encryption

Information is captured on the device and synchronized to the web application in a 'store and forward' manner. All information is encrypted using either 128-bit or 256-bit AES encryption dependending on the specific platform being used. Any communication across the 'wire' is always secured via 128-bit SSL (Secure Socket Layer over HTTP, otherwise known as HTTPS).

Data Center / Hosting Environment

The solution is hosted at a professionally managed, secure, tier 4 data center. Access to the facility is only allowed by authorized individuals with biometric identification and is guarded 24x7. All remote access to the servers is done only by authorized MDTech personnel and is logged. No sensitive information is moved away from this secure data center.

There are comprehensive backup and disaster recovery policies in place at the facility. Data is backed up incrementally on a nightly basis and stored for a minimum of six months.

PRIVACY AND SECURITY CHECKLIST FOR INFORMATION SYSTEMS

Common uses and disclosures	YES	NO	Comment
1. If patient information or access to the system will be provided to a 3rd party will a Business Associate agreement be signed with the 3rd party?	x		This is our standard practice, and we require one to be signed with all our customers.
2. If a support vendor will have a logon id into the system or will be removing hardware from the site for repair or replacement, will a Business Associate agreement be signed with the support vendor?	x		Yes, in addition no sensitive information is accessible to these personnel as everything is password protected beyond what is required for normal maintenance work.

Authentication and Authorization	YES	NO	Comment
3. Will all users have unique accounts?	x		
4. Will LDAP, NDS, Kerberos, or AD be used for authentication?			LDAP is supported, and through LDAP AD
5. Can the system be configured to require strong passwords and can admin change the strong password criteria as admin security standards change?		x	Partially implemented (support for length) slated for future release 3/1/14
6. Can the system be configured to expire user passwords periodically as defined by admin?		x	
7. Does the system provide a function to enable users to change their own passwords securely?	x		

Security Overview

8. Are passwords entered in a non-display field? 9. Are passwords encrypted during network transit? 10. Are passwords encrypted in storage?	x x x		Passwords aren't stored, only the hash
11. Are all attempted and successful logins logged? *Log should include date, time, user ID, network address*	x		Yes, this is a HIPAA requirement.
12. Can the system log users off after a defined period of inactivity?	x		Yes, this is currently set at 30 minutes.
13. Can users be given different levels of access within the app? *Ability to restrict access to particular application functions based on role assignment.*	x		Three roles are available, admin, physician, and collector. Specific permissions can be assigned for greater granularity.
14. Can users be restricted to access only data/records for which they are authorized? *Ability to restrict access to particular records based on role assignment.*	x		
15. Is authorization role based (rather than user ID based or managed by ACLs)?	x		Authorization is based both on roles and user id.
16. Can authorization be granted through a Enterprise Directory (i.e. AD, NDS, LDAP)?	x		Yes, for larger groups this is supported.
17. Can roles be tailored to our needs? *Customize roles to match our business processes*	x		Yes, roles can be customized. A requirements analysis can be done and our staff can configure this as part of your implementation.
18. Does the system provide security reports of users and access levels, so access can be reviewed periodically for appropriateness? *Reports that are easy to read by supervisors, not IT staff.*		x	This type of reporting is not built into the system but MDTech can provide these reports on an ad-hoc basis.
19. Can the system be configured to automatically disable user accounts or access privileges after a defined period of non-use?	x		Yes

Data Security	Yes	No	Comment
21. Is all network transfer of restricted and/or sensitive data encrypted, including between client workstations and application or database servers, between remote computers and application or database servers, etc?	x		Yes, - see high level description for specific technologies involved here.
22. Is all physical transfer of restricted and/or sensitive data encrypted?	x		
23. Will any restricted or sensitive data be stored by design, temporarily or otherwise, on end user workstations?		x	
24. Does the system provide appropriate controls to ensure data integrity? *Input validation, checksums of stored data, transaction redo logs*	x		
25. Will vendor/developer/system administrator staff who have privileged access be uniquely identified?	x		
26. Is activity of technical staff, including the Vendor/Developer, logged when performing system maintenance?	x		
27. Is User access to restricted and/or sensitive data logged?	x		
28. Does this logging specify the data element/record accessed?	x		
29. Does this logging specify the action taken upon the data? *View, modify, delete*	x		
30. Are there simple ways to generate meaningful and actionable reports from access audit logs? *Established audit reports (anomalies) readable by non IT staff.*		x	MDTech IT staff can generate this information on an ad hoc basis.
31. Can access to audit log reporting be restricted by role? *Compliance, Privacy or Security officer can run audit reports as needed without IT staff intervention. IT staff access can be restricted from user activity audit logs.*	x		
32. Is access to audit reports or the audit database logged?	x		

Security Overview

Data Security	Yes	No	Comment
33. Does the vendor/developer have and exercise a process to monitor for and test their software when security patches for the operating system are released?	X		

End User Device Security	Yes	No	Comment
34. Will anti-malware controls installed on workstations and portable devices continue to operate effectively (scanning and auto-updates) with this system?	x		
35. Will the automated patch management running on workstations and portable devices continue to operate effectively with this system?	x		
36. Is a password required to use the device?	x		
37. Does the device require a re-authentication after a settable period of inactivity?	x		
38. Can and will the system be configured to only permit the storage of restricted and sensitive information on secure servers, and not on end user workstations or portable devices?	x		
39. If sensitive or restricted data, temporary or otherwise, can be stored on the end user workstation or portable device, will it be effectively encrypted.	x		
40. Will all sensitive and restricted data transmitted between the end user workstation or portable device and a secured server be transmitted securely by encryption or otherwise over wired/wireless networks?	X		
41. Is there a mechanism to automatically update software on the device?	x		
42. Can information on the device be destroyed remotely if it is lost or stolen?	x		
43. Is the minimum amount of restricted and/or sensitive data stored on the device?	x		
44. Will the Unit or the vendor/developer provide end user support for the hardware and operating system of the portable device, to ensure it is configured securely and users know how to use it securely?	x		