Instructions: Check the appropriate column to indicate the application's security capabilities. Please provide any additional responses or detailed explanations of other compensating controls as comments. Please number your comments in the appropriate column and match the comment number with your detailed explanations at the end of this form. This questionnaire currently applies to healthcare applications and does not address the operating system or hardware controls.

Application Security Questionnaire

Application Name	Vendor	Version	Release Date

Application supports the following business functions:

Vendor Representative Contact Information	Name	Title	Department
	Company Name	Telephone #	e-mail

1.	ACCESS MANAGEMENT	Yes	No	N/A	Comment #
1.1	Does the application support integration with the enterprise identity management system?				
	a. If yes, indicate the alert (such as Directory Services, LDAP, Kerberos, etc.): _____ _____				
1.2	Is user authentication controlled by means other than user account and password or PIN?				
	a. If yes, indicate what other mechanisms are used (e.g. certificates, token, biometric, etc.): _____				
	Questions 1.3 through 1.8 apply to the use of passwords				
1.3	Does the application force "new" users to change their password upon first login into the application?				
1.4	Can the user change their password at any time?				
1.5	Can the system administrator enforce password policy and/or complexity such as minimum length, numbers and alphabet requirements, and upper and lower case constraint, etc.?				
1.6	Can the application force password expiration and prevent users from reusing a password?				
1.7	Is password transmission and storage encrypted and unviewable even to the system administrators?				
1.8	Can the application be set to automatically lock a user's account after a predetermined number of consecutive unsuccessful logon attempts?				
1.9	Does the application prohibit users from logging into the application on more than one workstation at the same time with the same user ID?				
1.10	Can the application be set to automatically log a user off the application after a predefined period of inactivity?				

1.11	Can access be defined based upon the user's job role? (Role-based Access Controls (RBAC))?				
	a. If yes, can application generate the list of users by job role?				
1.12	Can the application support the removal of a user's access privileges without requiring deletion of the user account?				
1.13	Does the application support a mechanism for allowing emergency access by a caregiver to a patient's electronic health information that is not included within their standard access privileges?				
	a. If yes, does the application capture and retain details pertaining to this action for review?				
	b. If yes, do the caregiver's access privileges revert back to the original setting upon next log-in?				
2.	**AUDIT CAPABILITIES**	**Yes**	**No**	**N/A**	**Comment #**
2.1	Is audit log tracking a feature available in the current version of this software application? *If yes, then continue with **2.2**; If no, continue with **3.0***				
2.2	Capturing user access activity such as successful logon, logoff, and unsuccessful logon attempts?				
	a. If yes, list the data elements contained in the audit log: _____ _____				
2.3	Capturing data access inquiry activity such as screens viewed and reports printed?				
	a. If yes, list the data elements contained in the audit log: _____ _____				
2.4	Capturing data entries, changes, and deletions?				
	a. If yes, list the data elements contained in the audit log: _____ _____				
2.5	Does the application time stamp for audit log entries synchronize with other applications and systems using NTP/SNTP?				
2.6	Are audit log reports available for the current version of this software application?				
	a. If yes, specify the types of reports: _____ _____				
	b. If yes, indicate if additional hardware or software (including any third-party software required to activate or utilize the audit logging and/or reporting feature: _____ _____ _____				
2.7	Can the audit log "data" be exported from the application for further processing (e.g. storage, analysis)?				
2.8	Indicate how audit log files are protected from unauthorized alteration: _____ _____				
2.9	Does the application allow a system administrator to set the inclusion or exclusion of audited events based on organizational policy and operating requirements or limits?				

2.10	Can the application continue normal operation even when security audit capability is non-functional? (For example, if the audit log reaches capacity, the application should continue to operate and should either suspend logging, start a new log or begin overwriting the existing log)				
3.	**SECURITY OF REMOTE ACCESS AND SUPPORT**	**Yes**	**No**	**N/A**	**Comment #**
3.1	Which connection method(s) are used to accomplish remote support?				
	a. Dial-up				
	b. Secure web tunneling				
	c. VPN Client (specify VPN technology method here):_____ _____				
	d. Business-to-Business VPN using IPSec				
	e. Other: _____ _____				
3.2	Identify which remote support applications are utilized and the security controls enabled: _____ _____ _____				
3.3	Is functionality built into the application which allows remote user access and/or control?				
3.4	If requested, can the application associate remote support activities with an individual employee of the vendor? (accountability)				
3.5	Do vendor support personnel have specific roles and accesses that control access to ePHI? *(See section 1.11)*				
3.6	Does the audit system log remote support connection attempts and remote support actions such as application or configuration modifications?				
4.	**PROTECTION FROM MALICIOUS CODE**	**Yes**	**No**	**N/A**	**Comment #**
4.1	Is the application compatible with commercial off the shelf (COTS) virus scanning software products for removal and prevention from malicious code?				
	a. If **no**, indicate what additional security controls are included with the application/system used to mitigate the risks associated with malicious code: _____ _____				
4.2	Does the application's client software operate without requiring the user to have local administrator level rights in order to run the application?				
5.	**CONFIGURATION MANAGEMENT AND CHANGE CONTROL**	**Yes**	**No**	**N/A**	**Comment #**
5.1	Are updates to application software and/or the operating system controlled by a **mutual** agreement between the support vendor and the application owner?				
5.2	Has the application been tested to be fully functional residing on its associated operating system/middleware platform configured with a recognized security configuration benchmark?				
	a. If yes, indicate the configuration benchmark:_____ _____ _____				

5.3	Can the operating system hosting the application (server or client) be updated by the user without voiding the application warranty or support agreement?				
	a. If no, will operating system changes, updates, and patches be provided by the vendor?				
5.4	Indicate how updates to the application are typically handled: _____				
5.5	Indicate how the application is certified to perform as intended with updates to the operating system and other helper applications (such as service packs and hotfixes) and how the customer is notified of this information.				
5.6	Do you provide documentation for guidance on establishing and managing security controls such as user access and auditing?				
6.	**DATA EXPORT AND TRANSFER CAPABILITIES**	**Yes**	**No**	**N/A**	**Comment #**
6.1	Does the application encrypt data before sending it over the Internet or an open network?				
	a. If yes, indicate the encryption used: _____				
6.2	Does the application encrypt data before storing on removable media such as backup tapes, CDs, DVDs, etc. or devices such as laptops, tablets, or computer workstation hard disk drives?				
	a. If yes, indicate the encryption used: _____				
6.3	Indicate the interfacing and format standards the application can accept or use for transferring data: (e.g., HL7 transaction formats, ANSI X.12 standards, CCOW, etc.): _____				
6.4	If the application includes a web interface, then identify the type(s) of secure connection supported: _____				
7.	**OTHER CAPABILITIES**	**Yes**	**No**	**N/A**	**Comment #**
7.1	Does the application maintain a journal of transactions or snapshots of data between backup intervals?				
7.2	Can the system administrator reconfigure to nonstandard port assignments other than the list of registered ports published by IANA?				
7.3	Does the application provide for integration into standard network domain structures?				
7.4	Has the application security controls been tested by a third party?				
7.5	Does the application have ability to run a backup concurrently with the operation of the application?				
7.6	Does the application include documentation that explains error or messages to users and system administrators and information on what actions required?				

Comments Section

Instructions: Use the space below for providing any additional responses, or detailed explanations of other compensating controls as comments. Please number your comments to match with comment number in column next to the question. You may comment on any future planned releases or updates that would enhance the security of the application.

Also, use the space below to list any other security threats, vulnerabilities, or risks that you are aware of that are not addressed in this checklist.

COMMENT #	COMMENTS

Disclaimer

This document is intended to assist healthcare providers in meeting their regulatory obligations regarding information security. It is the obligation of the users of this document (e.g., the healthcare provider) to employ all necessary and appropriate safeguards to meet their regulatory and organizational requirements. HIMSS does not assume any responsibility, written or implied, for the use or the content of this form.

References

SECTION	REFERENCE
1. ACCESS MANAGEMENT	1. CCHIT Security Criteria S4 *(Checklist question 1.13)*
2. AUDIT CAPABLITITIES	2. CCHIT Security Criteria S8.1, S10 & S11 *(Checklist questions 2.5, 2.9 & 2.10)*
3. REMOTE ACCESS AND SUPPORT	3. (Clinical and Laboratory Standards Institute. *Remote Access to Clinical Laboratory Diagnostic Devices via the Internet; Proposed Standard.* CLSI document AUTO9-P [ISBN 1-56238-560-7]. Clinical and Laboratory Standards Institute, 940 West Valley Road, Suite 1400, Wayne, Pennsylvania 19087-1898 USA, 2005.) 4. *REMOTE SERVICE INTERFACE – SOLUTION (A) Revision 2: IPSec over the Internet Using Digital Certificates*. Joint NEMA/COCIR/JIRA Security and Privacy Committee (SPC). Secretariat: NEMA (National Electrical Manufacturers Association) www.nema.org 1300 North 17th Street, Suite 1847, Rosslyn, VA 22209 USA 5. *Security and Privacy for Remote Servicing*. Joint NEMA/COCIR/JIRA Security and Privacy Committee (SPC). Secretariat: NEMA (National Electrical Manufacturers Association) www.nema.org 1300 North 17th Street, Suite 1847, Rosslyn, VA 22209 USA
5. CONFIGURATION MANAGEMENT AND CHANGE CONTROL	6. For configuration benchmarks, reference: Center for Internet Security http://www.cisecurity.org
6. DATA EXPORT AND TRANSFER CAPABILITIES	7. CCHIT Security Criteria S27 *(Checklist question 6.4)*
7. OTHER CAPABILITIES	8. CCHIT Security Criteria R3 and R11 *(Checklist questions 7.5 and 7.6)*

Cross-Reference with the Technical Safeguards of the HIPAA Security Rule

STANDARD AND/OR IMPLEMENTATION SPECIFICATION		QUESTIONS
Access Control	**§164.312(a)(1)**	**1.9, 1.11, 1.12**
Unique user identification *(Required)*	§164.312(a)(2)(i)	**1.1**
Emergency access procedure *(Required)*	§164.312(a)(2)(ii)	**1.13**
Automatic logoff *(Addressable)*	§164.312(a)(2)(iii)	**1.10**
Encryption and decryption *(Addressable)*	§164.312(a)(2)(iv)	**6.2**
Audit controls	**§164.312(b)**	**2.1 – 2.9, 3.6**
Integrity	**§164.312(c)(1)**	**4.1, 4.2, 7.4, 7.5**
Mechanism to authenticate electronic protected health information *(Addressable)*	§164.312(c)(2)	**7.1**
Person or entity authentication	**§164.312(d)**	**1.2 – 1.8**
Transmission Security	**§164.312(e)(1)**	**3.1 – 3.5**
Integrity controls *(Addressable)*	§164.312(e)(2)(i)	**6.3**
Encryption *(Addressable)*	§164.312(e)(2)(ii)	**6.1, 6.4**

Note: *Not all questions in this questionnaire are directly linked to the HIPAA Security Rule*

Definitions of Terminology

ANSI X.12	Uniform standards created by the American National Standards Institute (ANSI) for business transactions using electronic data interchange (EDI).
Authentication	The process of determining that an entity (someone or something) is the one claimed to be.
Authorization	The process of granting rights or access to systems, applications, or networks. Authorization determines who is trusted for a given purpose.
CCHIT	**Certification Commission for Health Information Technology (CCHIT)** - The industry-sponsored, federal government-endorsed commission which is developing criteria for certifying the functionality, security and interoperability of information technology products, starting with ambulatory care electronic medical records.
CCOW	HL7 provides the standard for clinical context management -- called CCOW -- that establishes the basis for ensuring secure and consistent access to patient information from dissimilar sources. CCOW was pioneered in 1996 by an independent consortium of vendors and healthcare providers *(CCOW formerly stood for Clinical Context Object Workgroup, but is now just an acronym)*
COTS	Commercial Off The Shelf software
Data elements	*(As used in this questionnaire in section 2)* Data elements refer to the auditable events contained in the audit trail such as successful, attempted, and failed logon, user logout, and user activities such as created, viewed, updated, and deleted data or records
Emergency access mechanism	A process within the application for allowing a caregiver immediate access to a patient's electronic health information in a life threatening situation which that caregiver would not normally have access to. (also known as: “Break the glass”)
ePHI	**Electronic Protected Health Information** – Any information which is created or received, that relates to the past, present, or future physical or mental health or condition of an individual or can be used to identify an individual that is transmitted or stored on electronic media. *(Note: ePHI must be safeguarded to protect it from unauthorized disclosure)*
HL7	**Health Level Seven** – Standards for electronic interchange of clinical, financial, and administrative information among healthcare computer systems.
IANA	(**Internet Assigned Numbers Authority**, www.iana.org) The Internet body that was responsible for managing Internet addresses, domain names and protocol parameters. It has been superseded by ICANN (Internet Corporation for Assigned Names and Numbers), which was formed in 1998. IANA was chartered by the Internet Society (ISOC) and Federal Network Council (FNC) and has been located at and operated by the Information Sciences Institute at the University of Southern California. **Source:** TechEncyclopedia (www.techweb.com/encyclopedia)
NTP / SNTP	(**Network Time Protocol**) A TCP/IP protocol used to synchronize the realtime clock in computers, network devices and other electronic equipment that is time sensitive. **Source:** TechEncyclopedia (www.techweb.com/encyclopedia)