NCHICA Vendor RFP Template for Meeting HIPAA Security Requirements

Prepared by the
NCHICA Privacy & Security Officials Work Group
and Security Work Group

Approved for Public Distribution
August 8, 2003

Introduction

The NCHICA Vendor RFP Template for Meeting HIPAA Security Requirements is intended to be used as a base document for inclusion in your Information Technology Request for Proposal (RFP) process. The questions in the RFP reflect the concerns of the NCHICA Privacy and Security Officials work group and the Security work group. It is intended to assist you in soliciting vendor responses to the Security issues you need to solve in order to achieve HIPAA Privacy and Security compliance. As stated earlier, this is a base document and can/should be modified to address your specific needs. The modifications can be additional questions or deletion of questions that are not applicable to your environment or have been previously resolved.

How to Use the Security Template

The template is comprised of four sections:

1. Standard

This section includes the requirement that needs to be addressed. It can take the form of a question or be a statement. The choice is yours.

2. Does Your System Comply?

This is where the responder provides a high level response to the Standard. The answers can be YES, NO, ALTernative. The responder MUST check one of the three boxes to indicate their position or solution capability. If the ALT box is checked the responder must provide a high level explanation of the ALTernative in the “Comments/Plans for Meeting Compliance” section. If there is supplemental information requested such as noted in the first standard under Password Controls, an answer MUST be provided.

3. Where in Your Proposal is the Solution Described?

In this section the responder inserts the reference to the details of the solution. It should be specific (e.g., volume, chapter/section, page and paragraph heading) as to where the answer can be found. Failure to provide the reference or an incorrect reference should be considered a NO answer. You will need to include the method by which this section must be responded to during the RFP process and explain that an incorrect or failure to provide a reference will be deemed a NO answer and will not be researched by your team. The objective here is to provide you and your evaluation team time to review and analyze the properly completed responses rather than spending time researching or looking for answers.

4. Comments/Plans for Meeting Compliance

In this section the responder provides any high level comments that may clarify a response in the “Does System Comply” section. It is especially important for responders to use this section to explain ALTernative checked responses. An ALTernative response can include a statement of future development or a solution that addresses the requirement however may not be a direct answer/solution to the requirement. This section MUST NOT be used for detailed descriptions of the response..

NCHICA Template for HIPAA Security Requirements

Review Date: _____ Conducted by: _____

Standards	Does System Comply?	Where in Your Proposal is the Solution Described?	Comments/Plans for Meeting Compliance
A. Password controls			
• **System enforced: specified minimum length password**	Yes:☐ No: ☐ ALT: ☐ Current Minimum: ___ Current Maximum: ___		
• **System enforced: user passwords automatically changed or revoked after a user defined period has passed**	Yes:☐ No: ☐ ALT: ☐ Current Change Interval: ___		
• **System enforced: users required to change their passwords following the initial set up or resetting of the password**	Yes:☐ No: ☐ ALT: ☐		
• **History of previously used passwords is maintained by the system to prevent reuse**	Yes:☐ No: ☐ ALT: ☐ Current Value: ___		
• **Users are provided the capability to change their own passwords at their discretion**	Yes:☐ No: ☐ ALT: ☐		
• **User id's are disabled after a specified number of consecutive invalid login attempts**	Yes:☐ No: ☐ ALT: ☐ Current # Attempts: ___		
• **System automatically logs users off after a specified period of inactivity**	Yes:☐ No: ☐ ALT: ☐ Current Auto logoff Time:___		
• **Passwords entered in a non-display field**	Yes:☐ No: ☐ ALT: ☐		
• **Passwords encrypted when routed over a network**	Yes:☐ No: ☐ ALT: ☐		
• **Passwords are encrypted in storage**	Yes:☐ No: ☐ ALT: ☐		
B. Security Administration			
• **System logs unauthorized access attempts by date, time, user id, device and location**	Yes:☐ No: ☐ ALT: ☐		
• **System maintains an audit trail of all security maintenance performed by date, time, user id, device and location and information is easily accessible**	Yes:☐ No: ☐ ALT: ☐		

Review Date: _____ Conducted by: _____

• **System provides security reports of users and access levels**	Yes:☐ No: ☐ ALT: ☐		
• **System provides a field(s) for personal information to be used for verification of users' identities for password resets and other maintenance (i.e. SSN, Mother's Maiden Name, DOB, etc). Fields used would not be a requirement**	Yes:☐ No: ☐ ALT: ☐		
• **System provides varying levels of access within the security application (i.e. Access to only password reset functions or Access to password reset function + Access to add & update users)**	Yes:☐ No: ☐ ALT: ☐		
• **System provides varying levels of access within the application**	Yes:☐ No: ☐ ALT: ☐		
• **System uses groups and unique user ids to define levels of access**	Yes:☐ No: ☐ ALT: ☐		
• **System provides the capability to place security controls on each system module and on confidential and critical levels within each module**	Yes:☐ No: ☐ ALT: ☐		
• **System provides capability to restrict access to particular records within the system, based on user id.**	Yes:☐ No: ☐ ALT: ☐		
• **System provides encryption of sensitive information transmitted over the network**	Yes:☐ No: ☐ ALT: ☐		
• **Security features comply with Federal (HIPAA), State and JCAHO health information standards for data integrity, confidentiality, auditing, and availability**	Yes:☐ No: ☐ ALT: ☐		
C. Activity Logging			
• **System logs unauthorized access attempts by date, time, user id, device and location**	Yes:☐ No: ☐ ALT: ☐		
• **System maintains an audit trail of all security maintenance performed by date, time, user id, device and location and information is easily accessible**	Yes:☐ No: ☐ ALT: ☐ Number of days kept: ___		

Review Date: _____ Conducted by: _____

• **System logs all accesses (including inquiry, which is required by HIPAA) to patient information**	Yes:☐ No: ☐ ALT: ☐		
• **System has auditing capabilities for both online or batch reporting. Can also be exported into Word, Excel, or other leading industry tools.**	Yes:☐ No: ☐ ALT: ☐		
• **Can logs be archived and recalled as needed?**	Yes:☐ No: ☐ ALT: ☐ Archive methods: ☐ Tape ☐ Disk ☐ Other		
D. Networking and Compatibilities			
• **Does your solution support external data transmission? Please indicate the method(s) supported.**	Yes:☐ No: ☐ ALT: ☐ Methods: ☐ FTP ☐ Fax ☐ Email ☐ File Copies (CD, Diskette, etc) ☐ Browser applications ☐ Tape media ☐ Other:		
• **For externally electronically transmitted information, can the solution support encryption and data protection?**	Encryption: Yes:☐ No: ☐ ALT: ☐ Data Protection: Yes:☐ No: ☐ ALT: ☐		
• **Can the system be accessed remotely (i.e., dialup, internet, etc.)**	Yes:☐ No: ☐ ALT: ☐ Methods: ☐ Dialup ☐ Internet ☐ Internet VPN ☐ Wireless		
• **Is the system compatible with?**	☐ Anti Virus software; Yes:☐ No: ☐ ALT: ☐ Please provide product specifics. ☐ Terminal Server:_____ Yes:☐ No: ☐ ALT: ☐		