

HITRUST Security Configuration Packs Methodology - Electronic Medical Records

March 2009

HITRUST is continuing our collaboration with the industry to define and provide benchmarks, assessment tools, leading practices and other services to ensure the appropriate implementation of required security controls by healthcare organizations. These materials, available in conjunction with the CSF and HITRUST Central (www.HITRUSTcentral.net) are the result of a consensus-building process that involves security experts from healthcare organizations, information technology vendors and professional services firms. A priority focus for HITRUST is the development of Security Configuration Packs for applications. These packs will address a significant void in the industry around clear direction for securing critical enterprise applications, such as electronic medical record systems.

The healthcare industry has unique challenges that require adapting generally accepted security practices to address the industry's specific requirements. One of these challenges for the industry is mitigating the risk related to security exposures with critical enterprise applications. The packs are integrated with the CSF, so organizations understand how to configure systems to comply with industry requirements. HITRUST is also collaborating with technology companies (e.g., vulnerability scanner products) and service providers (e.g., security firms) to integrate this information in their products and services to enhance the applicability of their solutions to healthcare organizations. These packs and associated tools are critical resources for healthcare organizations to enhance their security posture in an effective and sustainable manner.

The Security Configuration Packs will include the following type of information:

- General installation architecture considerations (e.g., placement on the network)
- Instructions for recommended configuration security settings in the application
- Instructions for recommended hardening of the application platform, e.g.
 - o operating system
 - o web server
 - o database
 - o interfaces
- Instructions for maintaining and monitoring configuration settings
- Instructions for configuring user privileges

The intended audience for the security configuration packs includes security architects, system integrators, system and security administrators, auditors, security technology vendors and professional service firms.

We are beginning the development of CSF security configuration packs for Electronic Medical Record systems with organizations using the systems. We prefer to develop these in collaboration with application vendors and believe this initiative can be a win/win for your customers, your organization and HITRUST. As an application vendor, your involvement will include:

- Providing expertise around your application
- Providing reference information to the team developing the documents
- Working in conjunction with a professional services firm, HITRUST and customers to develop the packs
- Subscribing to HITRUST Central for access to the CSF
- Moderating a forum for customer questions around the use of the pack

If you are interested in working with HITRUST to develop a security configuration pack for your system, please email info@HITRUSTalliance.org or call (469) 587-2200.

Security Configuration Pack Template: Electronic Medical Records

1 Introduction and Background

This section will include background information for:

- Organizations that contributed to the development of the configuration pack
- The product company
- Overview of the particular products

2 **[INSERT SYSTEM]** Security Configuration Pack

Products and services and related versions included in this document:

#	Product/Service Name	Product/Service Module	Version	Notes
1	Inpatient EMR	CPOE	v.2	

2.1 General deployment architecture considerations

- General information about the system architecture. Description of all components, including:

Product Ref	Component Type	Component Description	Version
1	Operating System	Microsoft Server	2008
1	Web Server		
1	Database		
1	Interface Engine		

2.2 Overall System Architecture Diagram

<DIAGRAM INSERTED HERE>

2.3 Architecture considerations regarding deployment

- Recommendations for network segmentation if applicable
- Recommendations for interface security if applicable
- Recommendations for use of encryption if applicable

2.4 Environmental Considerations

These security controls are related to organization policies and procedures, additional recommended services, solutions, devices or applications to support the system and ensure an appropriate level of control (commonly referred to as defense-in-depth).

2.5 Intended Audience

- Security architects
- System integrators
- System administrators
- Security administrators
- Auditors
- Security technology vendors
- Professional service firms.

2.6 Support Team Contact Information

Organization	Name	Email	Phone	Location
HITRUST	Cliff Baker	Cliff.baker@HITRUSTalliance.net	678.595.8984	Atlanta, GA
HITRUST	Chris Hourihan	Christopher.hourihan@HITRUSTalliance.net	404.281.6505	Atlanta, GA

3 System Component Configurations

System Comp.	CSF Ctrl Ref.	CSF Imp. Lvl	Configuration Item	Action(s) / Parameter(s)	Comments	Ver.
Application Program	1.b	1	EXAMPLE Roles and Privileges	When dropping a user, ensure roles and privileges created by that user, if not required, are deleted.	If a user is dropped, ensure that the roles and privileges created by that user, if not required, are deleted. Dropping a user (i.e., DROP USER X CASCADE) doesn't delete roles and privileges created by the user.	10g, 9i
Web Server						
Database						

Operating System						
Network Service						

4 Alternate Controls

The following table documents any known control failures associated with the system:

Document any discovered control failures associated with the system. The control failures should be appropriately documented and submitted, with any known Alternate Controls, to the HITRUST Alternate Controls Committee for review.

Control Failure Type	HITRUST CSF Control Reference	Control Failure Description	SCAP Standard Reference (optional)	Alternate Control (optional)