

HITRUST Security Configuration Packs Methodology - Electronic Medical Records

March 2009

While information security threats and vulnerabilities are prevalent today, the healthcare industry has unique challenges that require adapting generally accepted security practices to address the industry's specific requirements. The stakes are high as the Institute of Medicine highlights in its recent paper on privacy: "breaches of an individual's privacy and confidentiality may affect a person's dignity and cause irreparable harm" and "[unauthorized disclosures] can result in stigma, embarrassment, and discrimination". One of these challenges for the industry is mitigating the risk related to security exposures with critical enterprise applications. In the most severe cases, these exposures may lead to a negative impact on the safety and the well being of patients or to the extended outage of healthcare services.

Unfortunately, healthcare organizations continue to share the spotlight of organizations that are routinely experiencing security breaches. Many of these breaches are the result of vulnerabilities in applications within the organization. Vulnerabilities are caused by software defects or the lack of technical security controls. Software defects are addressed by vendor patches. Weak technical security controls exist because software products do not include adequate security functions, or security functions do exist but are not appropriately configured by the organization. Examples of technical security controls include settings for passwords, encryption, or logging and monitoring.

Organizations also have very few reliable and consistent resources for determining the best possible configuration and maintenance of security in critical applications, such as electronic medical records. Additionally, organizations struggle with the most effective and secure placement of critical applications within their IT infrastructure.

HITRUST intends to address these issues by collaborating with the industry and professional service firms to develop Security Configuration Packs as a resource for organizations to leverage in configuring and maintaining security for these critical 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. Case studies performed by the Center for Internet Security found that 80-90% of known vulnerabilities can be mitigated by organizations implementing

configuration benchmarks. The federal government considers configuration management a critical component in enterprise security, even reducing the frequency of assessments when robust configuration management is in place.

The Security Configuration Packs will include the following types 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.,
 - operating system
 - web server
 - database
 - 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.

Security Configuration Pack Template for 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)