Information Technology Security Plan

This template is to be used as a guide in developing individual security plans for new and changing medical devices, applications and/or infrastructure systems.

This document is intended to document controls for reasonably anticipated threats and vulnerabilities. The evaluation of responses will be made throughout the process. UHIT Management will make a final review and risk decision.

- Note: Approval of a security plan does not provide any assurances that UHIT Systems, DBA, interface or other IT groups can immediately start your project.
- Purchases, Contracts and Implementation of new IT assets will not move forward without the completion of an IT Security Plan.
- Submission of a Security Plan does not necessarily guarantee acceptance of the product. Approval by UH IT management is still required.

- **Important:** Please start this effort by creating a Visio or other graphical workflow of the system. Include all points where information is created or accessed, mapping through appropriate network areas. Include the server/database/application and then diagram return paths if applicable. Finally, map the backup and recovery processes and include your diagram(s) either in the field specified in the plan or as an appendix item at the end of the plan. Please do **not** send diagrams as additional attachments.

The Security Plan will be completed before the system is migrated to production and/or before new systems or upgrades can be purchased. This template will also be used to document current systems, where such documentation does not already exist.

Note: For confidential or Restricted Data outsourcing UNMH requires all available third party security certifications/attestations (preferably based on standards such as: (ISO 27002, NIST 800-53, SSAE-16 SOC 2, OWASP, or equivalent) from the vendor that are applicable to the service / application under consideration. For payment card hosting, PCI DSS attestation and reports will be required.

1. If necessary, the vendor can submit a redacted copy of certifications to safeguard sensitive information.
2. UNMH reserves the right to request and review the vendor's third party certifications/attestations annually.
3. Any vendor who also partners with third parties that create, use, transmit, receive or store UNMH data are required to provide independent third party security certifications/attestations.

Please complete all sections of the plan. Contact the IT Security Office with questions at 272- 3282.

Questions for the vendor are colored Blue

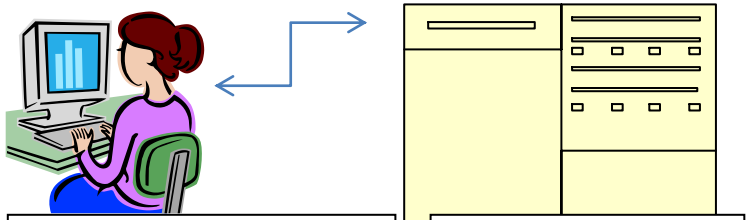
Questions for the UH Requestor are colored Green

Completed System Security Plans are UNM HOSPITALS Restricted (Internal Use Only). Handle accordingly and limit distribution per UNM Hospitals' Information Classification procedure. **Information System Security Plan** Please place Device or System Name here:	
Department Originator and Trusted Partner/Vendor Section. **The ITSecurityplan process requires that we be able to contact both the department representative and the vendor throughout the plan process. Please complete the section below as well as typing in the system or device name the row above.**	
Vendor Name and System Name:	☐ **System or device name:** ☐ **Version of your system (e.g. V 3.7):** ☐ **Vendor-Trusted Partner name:**
Request type:	☐ **New System, Application, etc.** ☐ **If medical device, please check this box!** ☐ **Upgrade to existing system, application or device** ☐ **RFP** ☐ **Other, please specify:**
Contact Information:	Department Initiator-Department Lead Contact Information: Name: E-mail: Best phone number for contact: Vendor/Trusted Partner Contact Information: Name: E-mail: Best phone number for contact:
Business Process Owner:	Who is the business process owner for this system (usually the Director of the Dept. requesting it)?
Location/Business Area:	Where will this system be used?
Notes:	Is there any additional information that you think might prove useful?

Completed System Security Plans are UNM HOSPITALS Restricted (Internal Use Only). Handle accordingly and limit distribution per UNM Hospitals' Information Classification procedure. **Information System Security Plan**

Please place Device or System Name here:

Department Originator and Trusted Partner/Vendor Section.
The ITSecurityplan process requires that we be able to contact both the department representative and the vendor throughout the plan process. Please complete the section below as well as typing in the system or device name the row above.

Overview of Data Flow *Diagram and Processes:* More than one data flow charts or diagrams may be used to properly describe the flow of information where necessary. **Note: This is a key requirement of the process.**	Vendor/Trusted Partner, please place data flow diagram in this section: (Please delete this example and put in your own data flow diagram). 
Brief Description:	Vendor please provides a brief description of your device, application, etc. What does it do and how does it do it?
Data Classification & Confidentiality Requirements:	What type of data is handled/processed by your system? ☐ **Confidential Level I** (ePHI, PII, etc.) Please specify patient identifiers e.g. Name, MRN, DOB Etc. here: ☐ **UH Restricted Level II** (information that is to remain inside UH systems) or ☐ **Unrestricted Level III** (deidentified or public)
Access Requirements and Restrictions:	**Does your system or device provided for role based access? If so, please provide as much detail as possible on how this is achieved:**
Security Logging and Monitoring:	Please describe logging abilities. For example, are security logs exported to a central log server and how is confidential-ePHI access logging accomplished (who did what and when, as required by HIPAA)?

Completed System Security Plans are UNM HOSPITALS Restricted (Internal Use Only). Handle accordingly and limit distribution per UNM Hospitals' Information Classification procedure. **Information System Security Plan** Please place Device or System Name here:	
Department Originator and Trusted Partner/Vendor Section. **The ITSecurityplan process requires that we be able to contact both the department representative and the vendor throughout the plan process. Please complete the section below as well as typing in the system or device name the row above.**	
	Business Process Owner: Who is designated to read logs in your unit?
Security Training:	What initial and ongoing training for your application or device is provided?
System Components:	Please describe the various components of your system and how they interact with each other. What protocols are used etc.? How is data in transit secured?
Incident Response Components:	How do you handle incidents, system compromises etc. if/when they occur? Do you have 24/7/365 support?
System Backups:	Who backs up the data associated with this system and how is it done?
Remote Access Requirements:	Do you require remote access to the system via VPN etc. in order to support, update or maintain this system? If so, how is this achieved?
Data Integrity:	What data integrity checking is conducted by this system?
Data Encryption:	a) How do you encrypt data in transit?

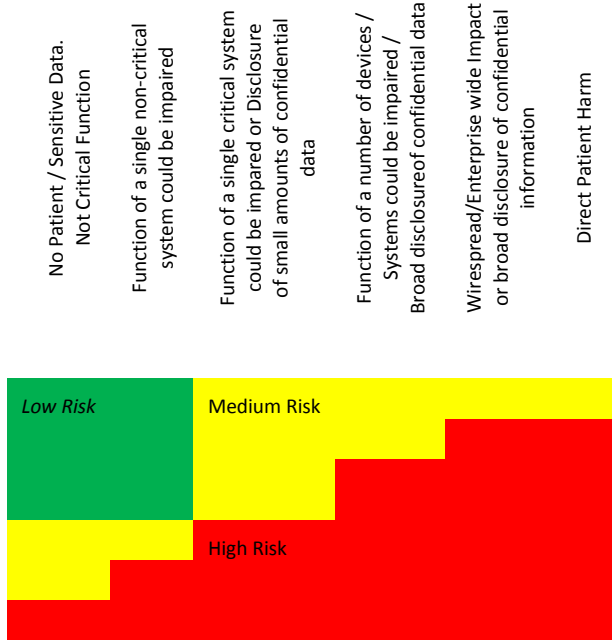
Completed System Security Plans are UNM HOSPITALS Restricted (Internal Use Only). Handle accordingly and limit distribution per UNM Hospitals' Information Classification procedure. **Information System Security Plan** Please place Device or System Name here: **Department Originator and Trusted Partner/Vendor Section.** **The ITSecurityplan process requires that we be able to contact both the department representative and the vendor throughout the plan process. Please complete the section below as well as typing in the system or device name the row above.**	
Note: to ensure HIPAA compliance, endpoint devices, data in motion and data at rest must be encrypted.	b) How do you encrypt data at rest? Do you support 3rd party encryption tools? If so, which ones?
Password Controls:	c) Please provide details of password complexity rules, failed logins lockouts, password history and other security measures available in the system:
Interfaces, Interconnections and Dependencies:	Does your system connect with others? If so what does it connect to and how does it do so?
Antiviral and Malware Protection:	What AV applications are approved for use with your system? (Our default is McAfee Enterprise v8.8 and this is our preferred option although others may also be acceptable).
OS and Application Patching:	How are the system, application and/or OS patched? How often does this occur? Who is responsible for this patching? Do you support continuous and current OS patching?

Completed System Security Plans are UNM HOSPITALS Restricted (Internal Use Only). Handle accordingly and limit distribution per UNM Hospitals' Information Classification procedure. **Information System Security Plan** Please place Device or System Name here:	
Department Originator and Trusted Partner/Vendor Section. **The ITSecurityplan process requires that we be able to contact both the department representative and the vendor throughout the plan process. Please complete the section below as well as typing in the system or device name the row above.**	
Third-party Applications & Patching:	Please list all 3rd party applications required by this system (e.g. Java, Active-X) and specify how they are patched? Do you support continuous and current patching of third party applications, including databases?
Physical Security:	Are any particular physical security measures required to safeguard this system?
Outsourcing Requirements. No exceptions:	If the data is stored anywhere other outside of UNMH's network, please specify where and provide independent 3rd party assessments (such as SSAE16 or SOC II) of your controls:
ICD-10 or 5010 Transaction Standards:	Do either standard apply to your system?
Vendor Name and Contact Information:	Please provide vendor contact information:
Version Number: 8.0	**Create Date: 9/17/2014**
Prepared By: Mgr. IT Security	**Issued By:**

Completed System Security Plans are UNM HOSPITALS Restricted (Internal Use Only). Handle accordingly and limit distribution per UNM Hospitals' Information Classification policies and guidelines.

Security Plan Risk

Likelihood of Attack	***Chance of problems***
Unconnected device with no interfaces	Improbable
Segmented / Connected device with controlled interfaces	Remote
Internally well connected devices with device based physical and IT controls	Occasional
Internally well connected device with clear physical and IT control gaps	Probable
Internet Facing device without any control deficencies (today)	Frequent
Internet facing device with control gaps	Assured



Risk Summary:

_____

_____

_____

Risk and Security Review

Director Network and Infrastructure approval Y/N comments: ,
Director PC Systems approval Y/N comments: ,

Administrator IT approval Y/N comments: ,
Manager IT Security approval Y/N comments: ,
Director Systems Development/Admin approval Y/N comments: ,
Director Clinical Systems approval Y/N comments: ,