HSC IT Project Security Requirements

This template is to be used as a guide in developing individual security assessments 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. HSC Management will make a final review and risk decision.**

- **Note: Approval of a security assessment does not provide any assurances that HSC 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 Assessment.**
- **Submission of a Security Assessment 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 assessment or as an appendix item at the end of the assessment. Please do **not** send diagrams as additional attachments.

Note: For confidential or Restricted Data outsourcing HSC requires all available third party security certifications/attestations (preferably based on standards such as: (ISO 27002, HITRUST, 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. If necessary, the vendor can submit a redacted copy of certifications to safeguard sensitive information. HSC reserves the right to request and review the vendor's third party certifications/attestations annually. Any vendor who also partners with third parties that create, use, transmit, receive or store HSC data are required to provide independent third party security certifications/attestations.

Please complete all sections of the assessment. Contact the IT Security Office with questions at 272- 8275.

Questions in RED are questions for the Vendor and or requester to answer for ITSEC. These are ITSEC follow-up questions for the vendor.

HSC IT Project Security Requirements

Security Requirement (Controls)	Detailed Information
Help.HSC Ticket #	< >

Contacts			
	Requestor (HSC/UNMH)	**Business Owner (HSC/UNMH)**	**Vendor – Technical**
Name	< >	< >	< >
Title	< >	< >	< >
Department	< >	< >	< >
Phone	< >	< >	< >
Email	< >	< >	< >

Vendor/System Details	
Vendor Name	< >
System Name	< >
Application name	< >
System version	< >
What does this system do?	< >

Request Type	
New System, Application, etc.	☐ < >
If medical device, check this box!	☐ < >
Upgrade existing system, application, etc.	☐ < >
Data transfer only (Web or portal)	☐ < >
RFP	☐ < >
Other, please specify:	☐ < >

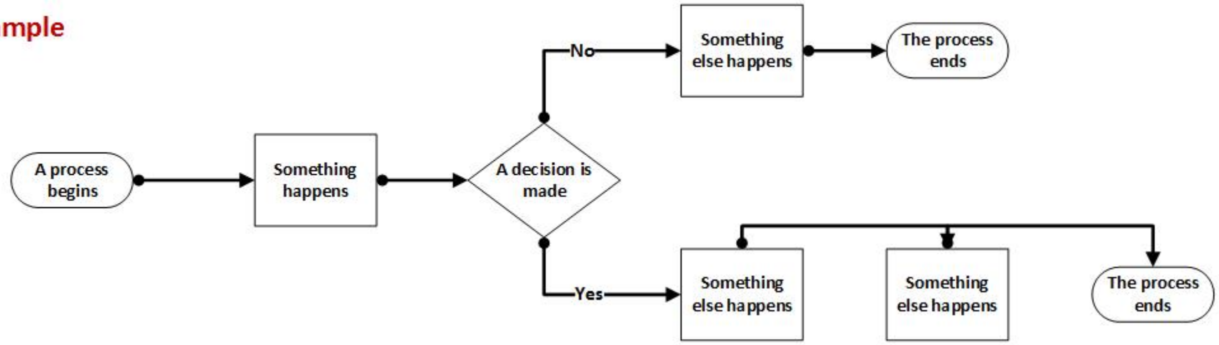
Identification of Roles	
System Administrator:	< >

Security Requirement (Controls)	Detailed Information
Application Administrator:	< >
Backup System Administrator:	< >
Summary of Hardware/Software	
Hardware	< >
Software Operating system? i.e. Windows 7 or 10, Windows Server 2008 or 2012 Any vendor or third party software on the system (e.g. Java, Adobe, etc.)	< >

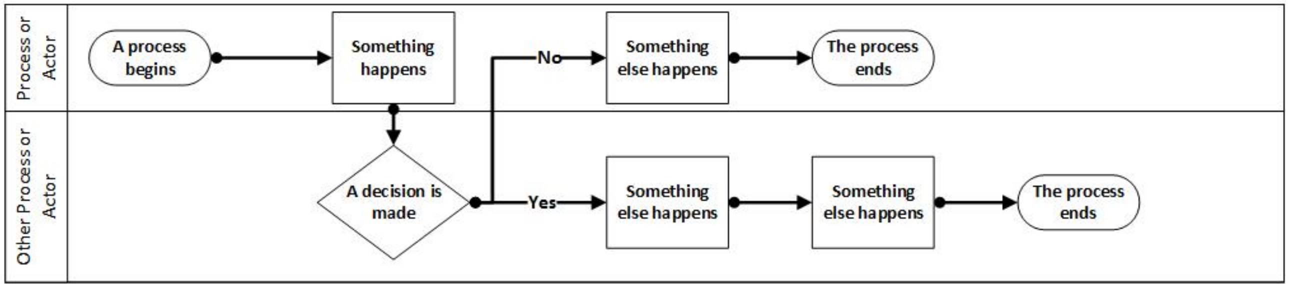
Overview of Data Flow Diagram and Processes

Where necessary, more than one data flow chart or diagram may be used to properly describe the flow of information.

Example



Example



HSC IT Project Security Requirements

Data Classification & Confidentiality Confirmation (verify from cover sheet) What type of data is handled/processed by your system?	
Data Sharing?	□ < >
Research Data?	□ < >
Pre-approved data in/out?	□ < >
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)	□ < >
Unrestricted Level III (de-identified or public)	□ < >
Interfaces, Interconnections and Dependencies	
Connections to any existing HSC systems? (Cerner, Active Directory accounts)	< >
Remote Access Requirements and Restrictions (Append information to data flow)	
Define your remote access requirements, (RDP, SSH, etc.)	< >
Account creation, modification, deletion, and review	
Please provide details of your procedure/policy	< >
Passwords Controls	
Please provide details of password complexity rules, failed logins lockouts, password history and other security measures available in the system:	< >
How do you ensure Data Integrity How do you ensure the confidentiality, integrity, and availability of information collected and utilized by this system?	

Confidentiality	< >
Integrity	< >
Availability	< >
Data Encryption To ensure HIPAA compliance, endpoint devices and confidential data in motion and at rest must be encrypted to a recommended standard (AES 256, TLS1.1). See NIST Standards	
Can the system be encrypted with MacAfee Encryption software?	□ < >
Can data be encrypted at rest?	□ < >
Can data be encrypted in motion?	□ < >
Security Logging and Monitoring	
What type of Logs does the system create/transmit (Syslog and specialized logs)?	< >
What is the frequency of Log review	< >
Who reviews these logs	< >
System Backups	
Who performs system Backups?	< >
What type of backup software/hardware is utilized?	< >
Antiviral and Malware Protection	
Is MacAfee AV compatible with your systems, if not, what products do you support?	< >
OS and Vendor Applications Patching	
What is you patching policy/procedure?	< >
Please specify Department or IT unit responsible for patching?	< >

HSC IT Project Security Requirements

Third-party Applications & Patching	
How are other software patches (Adobe, browser plugins, etc.) handled?	< >
Incident Response Components	
Which organization is the primary interface for security Incidents, or other incidents to the system?	< >
Disaster Recovery Process/Options	
What are the Disaster Recovery plans/processes failover and backup services for this system?	< >
Physical Security	
Are there any special physical security requirements (cameras, key-card access to system, etc.)?	< >
Outsourcing Requirements (Answer required)	
Do you outsource any part of this system to a Cloud or other organization? Do you keep all data in your organization or is it outsourced to a cloud or other company (US or outside of US)?	< >
ICD-10 or 5010 Transaction Standards	
Do ICD-10 or 5010 Transaction Standards apply?	< >
Security Training	
Which organization provides Security training for this product?	< >

FOR IT AND APPROVER USE ONLY

1. THREATS/VULNERABILITIES FOR SECURITY PLAN CONTROLS (THREATS TO UNMH NETWORK OR DATA)

SUMMARY OF IDENTIFIED VULNERABILITIES/THREATS			
Vulnerability/Threat	**Mitigation Status** (Has mitigation been completed or recommended (plan needed))	**Likelihood**	**Impact**
Vulnerability/Threat 1: < >	< >	Likelihood	Impact
Recommended Mitigation 1: < >	< >	Likelihood	Impact
Vulnerability/Threat 2: < >	< >	Likelihood	Impact
Recommended Mitigation 2: < >	< >	Likelihood	Impact
Vulnerability/Threat 3: < >	< >	Likelihood	Impact
Recommended Mitigation 3: < >	< >	Likelihood	Impact
Vulnerability/Threat 4: < >	< >	Likelihood	Impact
Recommended Mitigation 4: < >	< >	Likelihood	Impact

The calculation for this table is: Likelihood=2, Impact=2 Mitigations=4
Multiply likelihood score times impact score to indicate the risk score (2x2 = (4 is the risk score))
Multiply all the risk score totals by the number of mitigations (4 mitigations times 4 Risk score = 16)
Then divide the total risk score by the number of mitigations: (16 is the risk score divided by 4 mitigations = 4 for the Risk level).

2. IMPACT RANKS

There must be a defined threat listed above. **Threats** are HIGH **impact** by default. If NONE of the descriptors apply to a threat, it may be downgraded to a lower impact.

Low(1)	• Will have no effect on Patient / Sensitive Data. • Will have no loss of tangible assets or resources.

	• No personally identifiable data
Medium(2)	• May result in the loss of limited tangible assets or resources; • May reduce organization image, or slightly reduce an organization's mission, reputation, or interest • Will not result in human injury. • Will not result in loss of ePHI or PII in excess of 500 records • Will have no effect on core business operations
High(3)	• May result in the highly costly loss of major tangible assets or resources • May significantly violate, harm, or impede an organization's mission, reputation, or interest • May result in human death or injury. • May result in loss of ePHI or PII in excess of 500 records • System availability loss causes critical core business operations to not function or be unavailable.

3. SOURCE OF EXPLOIT

External (Internet Facing)	Y or N < >	If yes, there are significantly more threats that may exploit any vulnerabilities found in plan.
Internal (e.g. Accidental: user or privileged user makes mistakes affecting data integrity).	Y or N < >	Are controls in place to mitigate vulnerabilities found that could come from internal network or accidental mistakes?

4. LIKELIHOOD RANKS

Low(1)	• No Vulnerabilities found during review process • This vulnerability is theoretical, but there is no know method of exploitation • Mitigating controls make this threat's vulnerability impossible or highly unlikely to exploit using any known technique
Medium(2)	• Proof-of-concept reports exist, but not publicly available • Requires multiple steps to exploit • Only available to advanced attackers • Mitigating controls make this threat's vulnerability hard to exploit
High(3)	• Scattered reports are publicly available • Security controls are not layered or completely effective • Some automated tools can exploit the vulnerability for this threat

	- Mitigating controls are not completely effective
Very High(4)	- Reports of this vulnerability are reported publicly - Automated tools can scan for an exploit the underlying vulnerability for this threat - Key security controls missing - No mitigating controls in place to reduce this likelihood

5. RISK SCORE MATRIX

Risk Score Matrix		**Impact**		
		Low	**Medium**	**High**
Likelihood	**Low**	1	2	3
	Medium	2	4	6
	High	3	6	9
	Very high	4	8	12

Note 1: When calculating risk use the above numbers for assigning risk totals:
Green 1-3 risk is Low, Yellow 4 risk is Medium and Red 6-12 risk is High.

Note 2: When the ePHI data fields are limited to only MRN, the risk is “limited risk". The impact medium (2) and the likelihood would have to be low (1) or medium (2). Risk (2) × (2) = (4) Medium.

Definition: Risk is the combination of Probability-likelihood of and its consequences-impact (Impact is calculated first using Table 2. Then the probability-likelihood is calculated from Table 4.

Impact * Likelihood = Risk for each threat or vulnerability found the above plan.

6. SUMMARY AND APPROVALS

Security Analyst Name: < >
Security Analyst/Risk Summary: < >
Security Review Date: < >

Security Manager Name: < >
Security Manager Summary: < >
Security Review Date: < >

The following approvals must be recorded:

Director Network and Infrastructure
Approval: Y or N Comments: < >,

Director PC Systems
Approval: Y or N Comments: < >,

Administrator IT
Approval: Y or N Comments: < >,

Manager IT Security
Approval: Y or N Comments: < >,

Director Systems Development/Admin
Approval: Y or N Comments: < >,

Director Clinical Systems
Approval: Y or N Comments: < >,