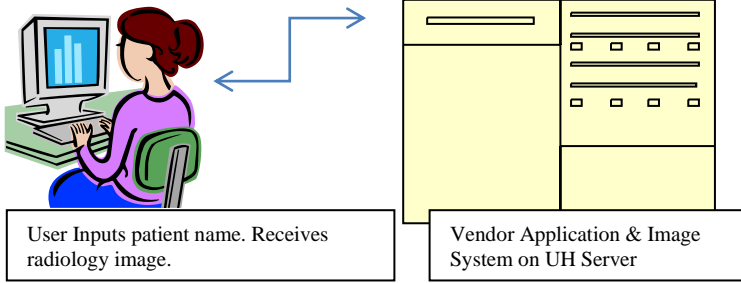


HSC IT Project Security Requirements

Security Requirement	Detailed Information
Requester Name: Name, Title, Department, Contact information, Help.HSC Ticket #	
Vendor Name, System Name, Application name, IP Address (if known)	
Summary of Hardware: Software Operating System, Vendor Application Software, and Third-Party Software	
Enterprise IT Services: (i.e., desktop, application, networking, and systems services. Include a list and explanation of firewall port exceptions)	
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.	Vendor/Trusted Partner, please place data flow diagram in this section: (Please delete this example and put in your own data flow diagram). 

HSC IT Project Security Requirements

Data Classification & Confidentiality Confirmation:	Data Classification Here: (Verify from cover sheet)
Interfaces, Interconnections and Dependencies:	
Access Requirements and Restrictions: (Append information to data flow)	
System Components: Any additional System Components required: (i.e., printers, scanner, camera, SAN, etc.)	
Data Integrity:	
Data Encryption: Note: to ensure HIPAA compliance, endpoint devices, data in motion and data at rest must be encrypted.	
Security Logging and Monitoring:	

HSC IT Project Security Requirements

System Backups:	
Antiviral and Malware Protection:	
OS and Application Patching:	
Third-party Applications & Patching:	
Incident Response Components:	
Physical Security:	

HSC IT Project Security Requirements

Outsourcing Requirements. (Answer required)	
ICD-10 or 5010 Transaction Standards:	
Security Training:	

HSC IT Project Security Requirements

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

Security Analyst Name:
Security Analyst Summary:

Security Manager Name:
Security Manager Summary:

HSC IT Project Security Requirements

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

IMPACT RANKS

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)	<ul style="list-style-type: none"> Will have no effect on Patient / Sensitive Data. Will have no loss of tangible assets or resources;
Medium(2)	<ul style="list-style-type: none"> 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)	<ul style="list-style-type: none"> 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.

HSC IT Project Security Requirements

Threats are **HIGH likelihood** by default. If **NONE** of the descriptors apply to a threat, it may be downgraded to a lower likelihood

Low(1)	<ul style="list-style-type: none"> • 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)	<ul style="list-style-type: none"> • 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)	<ul style="list-style-type: none"> • 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)	<ul style="list-style-type: none"> • 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

The following approvals must be recorded:

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: ,