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. UNMH Management will complete a final review and risk decision. The intake process and submission to the Management Review Team can take 1-2 months, based on the vendor’s ability to answer and respond their questions in this document.

* Note: Approval of a security assessment does not provide any assurances that UNMH/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 UNMH 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. Please do **not** send diagrams as additional attachments.

Note: For confidential or Restricted Data outsourcing UNMH/HSC requires all available third party security certifications/attestations (preferably based on standards such as: (ISO 27002, HITRUST, NIST 800-53, SSAE-18/SOC3, OWASP, or equivalent 3rd party assessment) 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. UNMH reserves the right to request and review the vendor's third party certifications/attestations annually. **Any vendor who also partners with third parties (AWS, ETC.) that create, use, transmit, receive or store UNMH/HSC data are required to provide independent third party security certifications/attestations for their Product, not just the AWS SOC3.** The vendor may require an NDA between their organization and UNMH/HSC in order to provide the security information request ion in this document, which UNMH.

**Please complete all sections of the assessment. All sections marked in blue and labeled R, are to be completed by the UNMH Requester. All sections marked in yellow and labeled V, are to be completed by the Vendor. Follow up questions in red are questions for the vendor and or requester to answer. Contact UNMH Cyber Security with questions at** **ITSecurityPlan@salud.unm.edu****.**

**UNMH is required By HIPAA LAW to utilize** ISO **27002, HITRUST, NIST 800-53, SSAE-18/SOC3, OWASP other Cybersecurity Frameworks and publications to build a cybersecurity infrastructure to secure our operational environment. We must ensure our vendors follow the same practices for all hardware/software/services. This document is based on our belief that the vendor follows all of these processes and industry best practices.**

| **Q#** |  | **IT Project Overview** | **Detailed Information** |
| --- | --- | --- | --- |
| **1R** | [ ] **Check if Complete** | **R****W** | Cherwell Ticket # | < > |
| 2R | [ ] **Check if Complete** | Security team assigned: | [ ]  UNMH [ ]  HSC [ ]  UNMMG [ ]  UNMSRMC |
|  |  | **Contacts** |
|  |  | **R****W** |  | **Requestor Info (UNMH/HSC)** | **Director, Dean, Chair, CEO that approved proposal or project** **(UNMH/HSC)** | **Vendor – Contact Info** |
| 3R | [ ] **Check if Complete** | Name: | < > | < > | < > |
| 4R | [ ] **Check if Complete** | Title: | < > | < > | < > |
| 5R | [ ] **Check if Complete** | Department: | < > | < > | < > |
| 6R | [ ] **Check if Complete** | Phone: | < > | < > | < > |
| 7R | [ ] **Check if Complete** | Email: | < > | < > | < > |
|  |  | **Vendor/System Details** |
| **1V** | [ ] **Check if Complete** | **V****W** | Vendor name: | < > |
| **2V** | [ ] **Check if Complete** | System name : | < > |
| **3V** | [ ] **Check if Complete** | Application name: | < > |
| **4V** | [ ] **Check if Complete** | System version: | < > |
| **5V** | [ ] **Check if Complete** | What does this system do? | < > |
|  |  | **What Type of Request is This? (**Check all that apply) |
| **8R** | [ ] **Check if Complete** | **R****W** | Medical device: (MDS2 must be provided) | [ ]  Yes [ ]  No [ ]  NA < > Notes |
| 9R | [ ] **Check if Complete** | New system, application, etc. | [ ]  Yes [ ]  No [ ]  NA < > Notes |
| 10R | [ ] **Check if Complete** | Is this an Upgrade? | [ ]  Yes [ ]  No [ ]  NA < > Notes |
| 11R | [ ] **Check if Complete** | Is this a repurchase of existing system/application currently for another Unit or Clinic? | [ ]  Yes [ ]  No [ ]  NA < > Notes |
| 12R | [ ] **Check if Complete** | Does this system use a Mobile application for deployment (Ipad-Droid) | [ ]  Yes [ ]  No [ ]  NA < > Notes |
| 13R | [ ] **Check if Complete** | Was this part of an RFP: | [ ]  Yes [ ]  No [ ]  NA < > Notes |
| 14R | [ ] **Check if Complete** | Is this a Cloud Based System? If yes please state type(s) | [ ]  Yes [ ]  No [ ]  NA < > Notes |
| 15R | [ ] **Check if Complete** | Other, please specify: | [ ]  Yes [ ]  No [ ]  NA < > Notes |
|  |  | **Overview of Data Flow Diagram and Processes**Please illustrate how data moves internally within our network between systems and users. List all servers/databases utilized and interfaces required to connect to existing UNMH/HSC systems or applications; like Cerner, PACS, etc. Where necessary, more than one data flow chart or diagram may be used to properly describe the flow of information. PLEASE REPLACE THIS DIAGRAM WITH YOURS |
| **6V** |  | **V****W** |  |
|  |  | **Identification of Roles**Please list the systems, or other clinical staff assigned to this role for UNMH. Include contact information**. (UNMH IT Systems Team Section)** |
| **16R** | [ ] **Check if Complete** | **R****W** | UNMH System Administrator: | < > Notes |
| **17R** | [ ] **Check if Complete** | UNMH Department Application Administrator: | < > Notes |
| **18R** | [ ] **Check if Complete** | UNMH Backup System Administrator: | < > Notes |
| **7V** | [ ] **Check if Complete** | **V****W** | Vendor System Administrator: | < > Notes |
| **8V** | [ ] **Check if Complete** | Vendor Department Application Administrator: | < > Notes |
| **9V** | [ ] **Check if Complete** | Vendor Backup System Administrator: | < > Notes |
|  |  | **Summary of Hardware/Software Being Purchased (UNMH IT Systems Team Section)** |
| **10V** | [ ] **Check if Complete** | **V****W** | List all Hardware & Peripherals (USB, DVDRW, Printers, Etc.) | < > Notes |
| **11V** | [ ] **Check if Complete** | List all Software: (OS Server/Workstation/Other): | < > Notes |
| **12V** | [ ] **Check if Complete** | Is this an Internet Facing System? | [ ]  Yes [ ]  No [ ]  NA < > Notes |
| **13V** | [ ] **Check if Complete** | Does this system require a web server to run on the system? (IIS, Apache) | [ ]  Yes [ ]  No [ ]  NA < > Notes |
| **14V** | [ ] **Check if Complete** | List all dependent third party software on the system: (Java, Adobe, etc.) | < > Notes |
| **15V** | [ ] **Check if Complete** | Does your system utilize a local or enterprise database? | [ ]  Yes [ ]  No [ ]  NA < > |
| **16V** | [ ] **Check if Complete** | Have you tested your website security with a tool such as Qualys SSL Labs? If so list your site rating. | [ ]  Yes [ ]  No [ ]  NA < > Notes |
| **17V** | [ ] **Check if Complete** |  | If you are a SAAS or Cloud provider, is this a Multi-Tenancy environment? | [ ]  Yes [ ]  No [ ]  NA < > Notes |
| **18V** | [ ] **Check if Complete** |  | If this is a Multi-Tenancy SAAS environment, is UNMH Data separate from all other clients? | [ ]  Yes [ ]  No [ ]  NA < > Notes |
|  |  | **Account Controls (UNMH IT Systems Team Section)** |
| **19V** | [ ] **Check if Complete** | **V****W** | Do you have role based access controls not AD controlled roles? | [ ]  Yes [ ]  No [ ]  NA < > Notes |
| **20V** | [ ] **Check if Complete** | Do you Limit system access to authorized users, system accounts or other accounts? | [ ]  Yes [ ]  No [ ]  NA < > Notes |
| **21V** | [ ] **Check if Complete** | Do you have separation of duties for support staff? | [ ]  Yes [ ]  No [ ]  NA < > Notes |
| **22V** | [ ] **Check if Complete** | Do you employ the principle of least privilege, including for specific security functions and privileged? | [ ]  Yes [ ]  No [ ]  NA < > Notes |
| **23V** | [ ] **Check if Complete** | Do you limit unsuccessful logon attempts? | [ ]  Yes [ ]  No [ ]  NA < > Notes |
| **24V** | [ ] **Check if Complete** | Do you provide privacy and security notices to UNMH? | [ ]  Yes [ ]  No [ ]  NA < > Notes |
| **25V** | [ ] **Check if Complete** | Do you use a session/screen lock to prevent access and viewing of data after period of inactivity? | [ ]  Yes [ ]  No [ ]  NA < > Notes |
| **26V** | [ ] **Check if Complete** | Do you Terminate a user session after a defined condition is met? | [ ]  Yes [ ]  No [ ]  NA < > Notes |
| **27V** | [ ] **Check if Complete** | Do you Monitor and control remote access sessions? | [ ]  Yes [ ]  No [ ]  NA < > Notes |
| **28V** | [ ] **Check if Complete** | Do you prevent reuse of identities for a defined period?Do you disable identities after a defined period of inactivity? | [ ]  Yes [ ]  No [ ]  NA < > Notes |
| **29V** | [ ] **Check if Complete** | Do you Store and Transmit Passwords with TLS or other cryptography | [ ]  Yes [ ]  No [ ]  NA < > Notes |
| **19R** | [ ] **Check if Complete** | **R** | Do you have a specific Account procedure/policy for your department? | [ ]  Yes [ ]  No [ ]  NA < > Notes |
| **20R** | [ ] **Check if Complete** | What is the frequency of account review by your department? | [ ]  Yes [ ]  No [ ]  NA < > Notes |
| **21R** | [ ] **Check if Complete** | Who is responsible for account management and review? | [ ]  Yes [ ]  No [ ]  NA < > Notes |
|  |  | **Passwords Controls (UNMH IT Systems Team Section)** |
| **30V** | [ ] **Check if Complete** | **V****W** | Provide details and/or policy for your software password complexity rules, failed logins lockouts, password history and other security measures available in the system: Can your system utilize 9-character passwords-This is the UNMH Standard | [ ]  Yes [ ]  No [ ]  NA < > Notes |
| **22R** | [ ] **Check if Complete** | **R** | How often will passwords be changed? | < > Notes |
|  |  | **OS and Vendor Application Patching (UNMH IT Systems Team Section)** |
|  |  |  |  | **Operating System** | **Application** | **Third Party Applications** |
| **23R** | [ ] **Check if Complete** | **R** | Who is responsible for patching? | < > UNMH< > Vendor | < > UNMH< > Vendor | < > UNMH< > Vendor |
| **24R** | [ ] **Check if Complete** | How often are patches applied? | < > Notes | < > Notes | < > Notes |
| **25R** | [ ] **Check if Complete** | What is the method for delivering patches? | < > Notes | < > Notes | < > Notes |
| **31V** | [ ] **Check if Complete** | **V****W** | How do you test patches/updates for malicious code before the patches/updates are deployed to UNMH/Vendor systems? | < > Notes |
| **32V** | [ ] **Check if Complete** | **V****W** | Please specify if your system has any current vulnerabilities. | < > Notes |
| **33V** | [ ] **Check if Complete** | **V****W** | Do you and/or can you utilize multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete? | [ ]  Yes [ ]  No [ ]  NA < > Notes[ ]  On Premise [ ]  Cloud |
|  |  | **System Backups (UNMH IT Systems Team Responses)** |
| **26R** | [ ] **Check if Complete** | **R** | Who performs system backups? | < > Notes |
| **27R** | [ ] **Check if Complete** | Who performs database backups? | < > Notes |
| **28R** | [ ] **Check if Complete** | What type of backup software/hardware is utilized? | < > Notes |
|  |  | **Interfaces, Interconnections and Dependencies (UNMH IT Clinical Applications Team Section)** |
| **29R** | [ ] **Check if Complete** | **R** | Connections to any existing UNMH/HSC systems? (Cerner, Active Directory accounts) | [ ]  Yes [ ]  No [ ]  NA < > Notes[ ]  On Premise [ ]  Cloud |
|  |  | **ICD-10 or 5010 Transaction Standards** |
| **34V** | [ ] **Check if Complete** | **V** | Do ICD-10 or 5010 Transaction Standards apply? | [ ]  Yes [ ]  No < > Notes |
|  |  | **Remote Access Requirements and Restrictions (UNMH IT Network Team Section)**UNMH/HSC only authorizes connections through SecureLink |
| **35V** | [ ] **Check if Complete** | **V** | Do you need remote access to UNMH Systems: (RDP, SSH, etc.). | [ ]  Yes [ ]  No If you answer no move to next section |
| **36V** | [ ] **Check if Complete** | Do you monitor and control remote access sessions? | [ ]  Yes [ ]  No [ ]  NA < > Notes[ ]  On Premise [ ]  Cloud |
| **37V** | [ ] **Check if Complete** | **V** | Do you employ cryptographic mechanisms to protect the confidentiality of remote access sessions? | [ ]  Yes [ ]  No [ ]  NA < > Notes[ ]  On Premise [ ]  Cloud |
| **38V** | [ ] **Check if Complete** | Do you utilize/route remote access via managed access control points? | [ ]  Yes [ ]  No [ ]  NA < > Notes[ ]  On Premise [ ]  Cloud |
| **39V** | [ ] **Check if Complete** | Do you authorize remote execution of privileged commands and remote access to security-relevant information? | [ ]  Yes [ ]  No [ ]  NA < > Notes[ ]  On Premise [ ]  Cloud |
|  |  | **Wireless Controls (UNMH IT Network Team Section)** |
| **40V** | [ ] **Check if Complete** | **V****W** | Does your system authorize wireless access prior to allowing such connections? | [ ]  Yes [ ]  No [ ]  NA < > Notes[ ]  On Premise [ ]  Cloud |
| **41V** | [ ] **Check if Complete** | Does your system protect wireless access using authentication and encryption? | [ ]  Yes [ ]  No [ ]  NA < > Notes[ ]  On Premise [ ]  Cloud |
| **42V** | [ ] **Check if Complete** | Control connection of mobile devices. | [ ]  Yes [ ]  No [ ]  NA < > Notes[ ]  On Premise [ ]  Cloud |
| **43V** | [ ] **Check if Complete** | Encrypt information on mobile devices and mobile computing platforms. | [ ]  Yes [ ]  No [ ]  NA < > Notes[ ]  On Premise [ ]  Cloud |
| **44V** | [ ] **Check if Complete** | Does your system verify and control/limit connections to and use of external systems? | [ ]  Yes [ ]  No [ ]  NA < > Notes[ ]  On Premise [ ]  Cloud |
|  |  | **Data Classification & Confidentiality Confirmation (UNMH IT Cybersecurity Team Section) Check all that apply** |
| **30R** | [ ] **Check if Complete** | **R****W** | Confidential Level I *(ePHI, PII, etc.)* | [ ]  < >If Level I is checked you must supply a SOC2/3, SSAE 18 or related documents. Not just AWS SOC3, but 3rd party assessment of your solution is required as well. |
| **31R** | [ ] **Check if Complete** | UNMH/HSC Restricted Level II *(information that is to remain inside UNMH/HSC systems)* | [ ] < > Notes |
| **32R** | [ ] **Check if Complete** | Unrestricted Level III *(de-identified or public)* | [ ] < > Notes |
| **33R** | [ ] **Check if Complete** | No data is collected | [ ]  < > Notes |
| **34R** | [ ] **Check if Complete** | Does your system/website/cloud service utilize UNMH EPHI or restricted data? *(If EPHI or restricted data is utilized, current security assessment such as SSAE-18 or other security certifications must be provided.)* | [ ]  Yes [ ]  No [ ]  NA < > Notes |
|  |  | **Data Sharing Between Organizations or Cloud (UNMH IT Cybersecurity Team Section)** |
| **35R** | [ ] **Check if Complete** | **R****W** | Do you share data outside UNMH? | [ ]  Yes [ ]  No [ ]  NA < > Notes |
| **36R** | [ ] **Check if Complete** | If data is shared outside UNMH- please attach more information: | [ ] < > Notes |
| **37R** | [ ] **Check if Complete** |  | Is UNMH Data in a Multi-Tenancy Cloud environment? | [ ]  Yes [ ]  No [ ]  NA < > Notes |
|  |  | **Type of Data Collected and where will it be Used (UNMH IT Cybersecurity Team Section)****Check all that apply** |
| **38R** | [ ] **Check if Complete** | **R****W** | Location of Data: | [ ]  UNMH [ ]  HSC [ ]  UNMMG [ ]  UNMSRMC [ ]  Vendor Cloud |
| **39R** |  | PII-EPHI | [ ]  |
| **40R** |  | Research: | [ ]  |
| **41R** |  | Student: | [ ]  |
| **42R** |  | Other: | [ ]  |
| **43R** | [ ] **Check if Complete** | Pre-approved data in/out: | [ ] < > Notes |
| **44R** | [ ] **Check if Complete** |  | Pre-approved data in/out to vendor cloud? | [ ]  Yes [ ]  No [ ]  NA < > Notes |
|  |  | **What EPHI/PII Restricted Data is Used (UNMH IT Cybersecurity Team Section)**If EPHI data is collected, check the appropriate boxes that indicate what will be stored, transmitted, or processed. **Check all that apply.** |
| **45R** |  | **R****W** | Social Security Numbers (SSNs): | [ ]  |
| **46R** |  | UNM ID Numbers (Banner IDs): | [ ]  |
| **47R** |  | Patient Name: | [ ]  |
| **48R** |  | Patient DOB: | [ ]  |
| **49R** |  | Patient Address: | [ ]  |
| **50R** |  | Patient Payroll/Financial Information: | [ ]  |
| **51R** |  | Patient grades/ advisement or tutoring records: | [ ]  |
| **52R** |  | Patient Health Information (MRN, Prescriptions, Patient Care/ Information: | [ ]  |
| **53R** | [ ] **Check if Complete** | Patient Credit Card Information: | [ ]  |
| **54R** | [ ] **Check if Complete** | Other: (Please specify) | [ ] < > Notes |
|  |  | **Records** |
| **55R** | [ ] **Check if Complete** | **R****W** | How many records does this system create per year? | [ ]  Less than 500 [ ]  More than 500 < > Notes |
| **56R** | [ ] **Check if Complete** | Where will the data be stored? | [ ]  UNMH/HSC Campus [ ]  Cloud < > Other |
|  |  | **Agreements (UNMH IT Purchasing Team Section)** |
| **45V** | [ ] **Check if Complete?** | **V** | Do you have a vendor contract and/or statement of work in place with UNMH? | [ ]  Yes [ ]  No [ ]  NA < > Notes |
| **46V** | [ ] **Check if Complete** | Do you have a signed Business Associates Agreement in place currently with UNMH after 3-2018? | [ ]  Yes [ ]  No [ ]  NA < > Notes |
| **47V** | [ ] **Check if Complete** |  |  |  |
|  |  | **Data Encryption**  **(UNMH IT Cybersecurity Team Section)**HIPAA compliance requires EPHI data be encrypted in motion, in transit, and at rest. Recommended Standard (AES 256, TLS1.2) |
| **48V** | [ ] **Check if Complete** | **V****W** | Can the workstation and server be encrypted with McAfee encryption software? | [ ]  Yes [ ]  No [ ]  NA < > Notes |
| **49V** |  | Do you encrypt the data from start to finish? | [ ]  Yes [ ]  No [ ]  NA < > Notes |
|  |  | **Security Logging and Monitoring (UNMH IT Cybersecurity Team Section)** |
| **50V** | [ ] **Check if Complete** | **V****W** | What type of logs does the system create/transmit? (Syslog and specialized logs.) | [ ]  NA < > Notes |
| **51V** | [ ] **Check if Complete** | Do you create and retain system audit logs for UNMH to monitor, analyze/investigate, and report unlawful or unauthorized system activity? | [ ]  Yes [ ]  No [ ]  NA < > Notes |
| **52V** | [ ] **Check if Complete** | Do you log user activities? | [ ]  Yes [ ]  No [ ]  NA < > Notes |
| **53V** | [ ] **Check if Complete** | Who is responsible for review and update logged events? | [ ]  UNMH [ ]  Vendor [ ]  NA < > Notes |
| **57R** | [ ] **Check if Complete** | **R** | What is the frequency of log review by your team? | < > Notes |
| **58R** | [ ] **Check if Complete** | Who is responsible for log review? | [ ]  UNMH Requesting Department [ ]  UNMH IT < > Notes |
|  |  | **Antiviral and Malware Protection (UNMH IT Cybersecurity Team Section)** |
| **54V** | [ ] **Check if Complete** | **V** | Is McAfee AV compatible with your system? If no, what AV products are supported? | [ ]  Yes [ ]  No [ ]  NA < > Notes |
|  |  | **Incident Response (UNMH IT Cybersecurity Team Section)** |
| **55V** | [ ] **Check if Complete** | **V****W** | Which organization is the primary method of communications for security incidents, or other incidents to this system? | [ ]  UNMH [ ]  Vendor [ ]  NA < > Notes |
| **56V** | [ ] **Check if Complete** | When an incident involving UNMH data is detected, when is UNMH Notified? | < > Notes [ ]  NA |
| **57V** | [ ] **Check if Complete** | Can you provide UNMH an Incident Response policy/procedure related to this system? Can you supply an IR report? | [ ]  Yes [ ]  No [ ]  NA < > Notes |
| **58V** | [ ] **Check if Complete** | Can you provide UNMH with a risk-disclosure of any IAAS/PAAS/SAAS facilities outside of US locations? | [ ]  Yes [ ]  No [ ]  NA < > Notes |
| **59V** | [ ] **Check if Complete** | Can you provide UNMH with audit record review, analysis, and reporting processes for investigation and response to indications unlawful, unauthorized, suspicious, or unusual activity in your cloud? | [ ]  Yes [ ]  No [ ]  NA < > Notes |
|  |  | **Disaster Recovery (DR) Process/Options (UNMH IT Cybersecurity Team Section)** |
| **59R** | [ ] **Check if Complete** | **R** | What Disaster Recovery plans/processes does your team have in case of failover? Do you have backup services for this system? Please provide DR documentation. | < > Notes |
| **60R** | [ ] **Check if Complete** | Does UNMH or the vendor deal with Disaster recovery? | [ ]  Yes [ ]  No [ ]  NA < > Notes |
| **60V** | [ ] **Check if Complete** | **V****W** | What is the Vendor’s DR plan for their application? | < > Notes |
| **61V** | [ ] **Check if Complete** | What DR rate/priority is UNMH in their vendor’s cloud? | < > Notes |
|  |  | **Physical Security (UNMH IT Cybersecurity Team Section)** |
| **61R** | [ ] **Check if Complete** | **R** | Are there any special physical security requirements (cameras, key-card access to system, etc.)? | [ ]  Yes [ ]  No [ ]  NA < > Notes |
|  |  | **Outsourcing Requirements (UNMH IT Cybersecurity Team Section)** |
| **62V** | [ ] **Check if Complete** | **V****W** | Do you outsource any part of this system to a Cloud or other organization? | [ ]  Yes [ ]  No [ ]  NA < > Notes |
| **63V** | [ ] **Check if Complete** | Do you keep all of UNMH’s data in your organization or is it outsourced to a cloud or other company (US or outside of US)? | [ ]  Yes [ ]  No [ ]  NA < > Notes |
|  |  | **Security Training (UNMH IT Cybersecurity Team Section)** |
| **64V** | [ ] **Check if Complete** | **V****W** | Who is responsible for providing training for this system? | [ ]  Vendor [ ]  UNMH [ ]  NA < > Notes |
| **65V** | [ ] **Check if Complete** | During Training, do you ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with using this software/system? | [ ]  Yes [ ]  No [ ]  NA < > Notes |

**FOR CYBERSECURITY AND APPROVER USE ONLY**

## 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).**

## **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.
 |

## **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
 |

## Source of exploit

|  |  |  |
| --- | --- | --- |
| External (Internet Facing) | [ ] No[ ] Yes | 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). | [ ] No[ ] Yes | Are controls in place to mitigate vulnerabilities found that could come from internal network or accidental mistakes? |

## 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.**

***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.**

## Summary and approvals

**Security Analyst Name:** < >

**Risk Scoring:**

**1) Impact versus Likelihood Score=**

**2) Internet-Facing Exploit Risk=** [ ] Yes[ ] No [ ] NA

**3) Vendor Soc2/3, SSAE18 Submitted for Vendor Assumed Risk:** [ ] Yes[ ] No [ ] NA

**4) Qualys SSL Labs Vendor Web Site Rating/Score=**  [ ] NA

**5) Data Classification:**

* **Responsible Party for EPHI or PII Data Security (Level 1):** [ ] Vendor[ ] Health Systems[ ] Both [ ] NA
	+ **If EPHI or PII Data Used, How Many Records:** [ ] <500 Records[ ] >500Records
* **Restricted Data Security (Level 2):** [ ] Vendor[ ] Health Systems[ ] Both [ ] NA
* **Unrestricted (Public) Data (Level 3):** [ ] Vendor[ ] Health Systems[ ] Both[ ] NA

**Security Analyst/Risk Summary:** < >

**Security Review Date:** < >

**Security Manager Name:** < >

**Security Manager Summary:** < >

**Security Review Date:** < >

 **The following approvals must be recorded:**

UNMH CIO Approval: [ ]  Yes [ ]  No < > Comments-Requirements

Executive Director IT Approval: [ ]  Yes [ ]  No < > Comments-Requirements

Director Clinical IT Systems: [ ]  Yes [ ]  No < > Comments-Requirements

Director Customer Service: [ ]  Yes [ ]  No < > Comments-Requirements

Manager Network Approval: [ ]  Yes [ ]  No < > Comments-Requirements

Manager PC Systems Approval: [ ]  Yes [ ]  No < > Comments-Requirements

Manager Cybersecurity Approval: [ ]  Yes [ ]  No < > Comments-Requirements