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/HSC Management will make a final review and risk decision.**

* **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/HSC 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 UNMH/HSC requires all available third party security certifications/attestations (preferably based on standards such as: (ISO 27002, HITRUST, NIST 800-53, SSAE-16, 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. UNMH/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 UNMH/HSC data are required to provide independent third party security certifications/attestations.

**Please complete all sections of the assessment R is for the UNMH Requester, V is for the Vendor. Contact the UNMH Cyber Security Office with questions at** [**ITSecurityPlan@salud.unm.edu**](mailto:ITSecurityPlan@salud.unm.edu)**. *The Former Web Plan is part of this document as well, please fill out the sections with a “W” in them (I.e. RW & VW).***

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

| **Security Requirement**  **(Controls)** | | **Detailed Information** | | |
| --- | --- | --- | --- | --- |
| **R**  **W** | Help.HSC Ticket # | < > | | |
| Date of plan submission: | < > | | |
| Date of implementation: | < > | | |
|  | Security team assigned: | UNMH  HSC  UNMMG  UNMSRMC | | |
| **Contacts** | | | | |
| **V**  **W** |  | **Requestor (UNMH/HSC)** | **Director, Dean, Chair, CEO that approved proposal or project** **(UNMH/HSC)** | **Vendor – Technical** |
| Name: | < > | < > | < > |
| Title: | < > | < > | < > |
| Department: | < > | < > | < > |
| Phone: | < > | < > | < > |
| Email: | < > | < > | < > |
| **Vendor/System Details** | | | | |
| **V**  **W** | Vendor name: | < > | | |
| System name : | < > | | |
| Application name: | < > | | |
| System version: | < > | | |
| What does this system do? | < > | | |
|  | What is the Impact to patient Care with the implementation/deployment of this system? | High  Medium  Low | | |
| **Request Type**  Check all that apply | | | | |
| **R**  **W** | New system, application, etc. | < > | | |
| Medical device: (MDS2 must be provided) | < > | | |
| Upgrade existing system, application, etc.: | < > | | |
| Data transfer only: (Web Portal) | < > | | |
| RFP: | < > | | |
| Cloud Based System UNMH to Vendor | < > Please enter details of about the data leaving UNMH Systems | | |
| Cloud Based System Vendor to UNMH | < > Please enter details of about the data entering UNMH Systems | | |
| Does this system require a Mobile application deployment | < > Please enter details of about the App, the mobile device platform and App security controls | | |
| Other, please specify: | < > | | |
| **Identification of Roles (**Please Add Contact Information**)** | | | | |
| **R**  **V** | UNMH & Vendor System Administrator: | < > | | |
| UNMH & Vendor Department Application Administrator: | < > | | |
| UNMH & Vendor Backup System Administrator: | < > | | |
| **Summary of Hardware/Software** | | | | |
| **V**  **W** | List all Hardware: | < > | | |
| List all Software: (OS Server/Workstation/Other): | < > | | |
| Is this an Internet Facing System? | < > Does this system require internet access? | | |
| Does this system require a web server running on the system? | < > Do you have OWASP Security Controls implemented? Do you require and support IIS server in our environment? | | |
| Does your system verify and control/limit connections to and use of external systems? | Implemented  Planned to Implement  NA | | |
| Does your system limit use of organizational portable storage devices on external systems? | Implemented  Planned to Implement  NA | | |
| Does your system control information posted or processed on publicly accessible systems? | Implemented  Planned to Implement  NA | | |
| List vendor application and dependent third party software on the system: (Java, Adobe, etc.) | < > | | |
| Does your system utilize our standard databases: (SQL 2012 or greater, oracle 11g or greater, Mysql 5.7 or greater) | < > | | |
| Does your product/system require Internet/Web Access? If so what site does your system need to access, please list all URLs: | < > | | |
| Have you tested your website security with a tool such as Qualys SSL Labs? If so list your site rating. (<https://www.ssllabs.com/index.html>) | < > | | |
| **V**  **W** | If you are a SAAS provider is this a Multi-Tenancy environment and is the data storage shared by any of our competitors? | < > | | |
| **V**  **W** | Do you monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls? | Yes  No < > Explain | | |
| **V**  **W** | Do you employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems based on NIST Cybersecurity Framework, SP-80053 R4, and SP800-52a? | Yes  No < > Explain | | |

|  |  |  |
| --- | --- | --- |
| **Overview of Data Flow Diagram and Processes**  Please illustrate how the data moves internally within our network/enterprise 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. | | |
| **V**  **W** |  | |
| **Data Classification & Confidentiality Confirmation**  What type of data is handled/processed by your system? | | |
| **R**  **W** | **Confidential Level I** (ePHI, PII, etc.)  If Level 1 data is chosen, the requirement documentation; you must supply is a SOC2, SSAE 16 or related documents | < >  If above checked please attach required document(s) to this Plan |
| **UNMH/HSC Restricted Level II** (information that is to remain inside UNMH/HSC systems) | < > |
| **Unrestricted Level III** (de-identified or public) | < > |
| Does your product/website/cloud service utilize EPHI or restricted data? (If EPHI or restricted data is utilized, current security assessment such as SSAE-16 or other security certifications must be provided.) | < > |
| **Data Sharing**  Will data be shared between the UNMH/HSC and a vendor or other entity? | | |
| **R**  **W** | No sharing allowed: |  |
| Yes, please attach more information: | < > |
| **Data Type**  (Select all that apply) | | |
| **R**  **W** | PHI: |  |
| Research: |  |
| Student: |  |
| Other: |  |
| Data Sharing: | < > |
| Pre-approved data in/out: | < > |
| **Data identifiers**  If EPHI data is collected, check the appropriate boxes that indicate what will be stored, transmitted, or processed. Check all that apply. | | |
| **R**  **W** | Social Security Numbers (SSNs): |  |
| UNM ID Numbers (Banner IDs): |  |
| Patient Name: |  |
| Patient DOB: |  |
| Patient Address: |  |
| Patient Payroll/Financial Information: |  |
| Patient Grades/ Advisement or Tutoring Records: |  |
| Patient Health Information (MRN, Prescriptions, Patient Care/ Information: |  |
| Patient Credit Card Information: |  |
| Other: (Please specify) | < > |
| **Number of Records** | | |
| **R**  **W** | < 500 total records created per year? |  |
| 500 or more total records created per year? |  |
| **Location of Data Use** | | |
| **R**  **W** | Globally: |  |
| UNMH/HSC Campus Only: |  |
| Department or Specific Staff Only, Other: (Please specify) | < > |
| **Agreement**  Do you have a sample vendor contract and/or statement of work? | | |
| **V** | No: |  |
| Yes, please attach: |  |
| **BAA**  Do you have a signed BAA? | | |
| **R** | No: |  |
| Yes, please attach: |  |
| **Interfaces, Interconnections and Dependencies** | | |
| **R** | Connections to any existing UNMH/HSC systems? (Cerner, Active Directory accounts) | < > |
| **Remote Access Requirements and Restrictions**  UNMH/HSC only authorizes connections through SecureLink. | | |
| **V** | Define your remote access requirements to UNMS Systems: (RDP, SSH, etc.) | < > |
| **V** | Do you monitor and control remote access sessions? | Implemented  Planned to Implement  NA |
| **V** | Do you employ cryptographic mechanisms to protect the confidentiality of remote access sessions? | Implemented  Planned to Implement  NA |
| **V** | Do you utilize/route remote access via managed access control points? | Implemented  Planned to Implement  NA |
| **V** | Do you authorize remote execution of privileged commands and remote access to security-relevant information? | Implemented  Planned to Implement  NA |
| **V** |  | Implemented  Planned to Implement  NA |
| **Wireless Controls** | | |
| **V**  **W** | Does your system authorize wireless access prior to allowing such connections? | Implemented  Planned to Implement  NA |
| **V**  **W** | Does your system protect wireless access using authentication and encryption? | Implemented  Planned to Implement  NA |
| **V**  **W** | Control connection of mobile devices. | Implemented  Planned to Implement  NA |
| **V**  **W** | Encrypt information on mobile devices and mobile computing platforms. | Implemented  Planned to Implement  NA |
| **V**  **W** | Does your system verify and control/limit connections to and use of external systems? | Implemented  Planned to Implement  NA |
|  |  |  |
| **Account Controls** | | |
|  |  |  |
| **V**  **W** | Do you follow NIST SP-800-171 for your software/system account controls in your software? | < > |
| How are user roles controlled? Do you have accounts/roles for all users and admins? Not AD defined, but software/application defined? | < > |
| **V**  **W** | Do you Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems)? | Implemented  Planned to Implement  NA |
| **V**  **W** | Do you limit system access to the types of transactions and functions that authorized users are permitted to execute.? | Implemented  Planned to Implement  NA |
| **V**  **W** | Do you control the flow of information in accordance with approved authorizations? | Implemented  Planned to Implement  NA |
| **V**  **W** | Do you separate the duties of individuals to reduce the risk of malevolent activity without collusion? | Implemented  Planned to Implement  NA |
| **V**  **W** | Do you employ the principle of least privilege, including for specific security functions and privileged? | Implemented  Planned to Implement  NA |
| **V**  **W** | Do you limit unsuccessful logon attempts? | Implemented  Planned to Implement  NA |
| **V**  **W** | Do you provide privacy and security notices consistent with applicable privacy rules? | Implemented  Planned to Implement  NA |
| **V**  **W** | Do you use session lock with pattern-hiding displays to prevent access and viewing of data after period of inactivity? | Implemented  Planned to Implement  NA |
| **V**  **W** | Terminate (automatically) a user session after a defined condition. | Implemented  Planned to Implement  NA |
| **V**  **W** | Monitor and control remote access sessions. | Implemented  Planned to Implement  NA |
| **V**  **W** | Do you use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts?  Do you employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts? | Implemented  Planned to Implement  NA |
| **V**  **W** | Do you prevent reuse of identifiers for a defined period?  Do you disable identifiers after a defined period of inactivity? | Implemented  Planned to Implement  NA |
| **V**  **W** | Store and transmit only cryptographically-protected passwords. | Implemented  Planned to Implement  NA |
| **R** | Please provide details of your UNMH Account procedure/policy: | < > |
| What is the frequency of account review by your department? | < > |
| Who is responsible for account management and review? (Please see Account Creation Policy: <https://hospitals.health.unm.edu/intranet7/apps/doc_management/index.cfm?document_id=286238>.) | < > |
| **Passwords Controls** | | |
| **V**  **W** | Please 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** | < > |
| **R** | How often will passwords be changed? | < > |
| **Data Integrity**  How do you ensure the confidentiality, integrity, and availability of information collected and utilized by this system? | | |
| **V**  **W** | 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. | | |
| **V**  **W** | Can the system be encrypted with MacAfee encryption software? | < > |
| Will data at rest be encrypted? What algorithm is used? | < > |
| Will data in motion be encrypted? What algorithm is used? | < > |
| **Security Logging and Monitoring** | | |
| **V**  **W** | What type of logs does the system create/transmit? (Syslog and specialized logs.) | < > |
| **V**  **W** | Does your system create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity? | Yes  No < > Explain |
| **V**  **W** | Does your system ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions? | Yes  No < > Explain |
| **V**  **W** | Who is responsible for review and update logged events? | Yes  No < > Explain |
| **V**  **W** | Do you correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity? | Yes  No < > Explain |
| **R** | What is the frequency of log review? | < > |
| Who is responsible for log review? Your Team or UNMH IT? | < > |
| **System Backups** | | |
| **R** | Who performs system backups? | < > |
| Who performs database backups? | < > |
| What type of backup software/hardware is utilized? | < > |
| **Antiviral and Malware Protection** | | |
| **V** | Is McAfee AV compatible with your system, if not, what AV products do you support? | < > |
| **OS and Vendor Applications Patching** | | |
|  | Wo is responsible for patching UNMH or vendor? | < > |
| **R** | What is your patching policy/procedure? | < > |
| How often are application patches applied? | < > |
| How often are OS patches applied? | < > |
| **V**  **W** | Please specify Department or IT unit responsible for OS patching? | < > |
| Please specify Department or IT unit responsible for application patching? | < > |
| **V**  **W** | Please specify if your product(s) have any current vulnerabilities or have any listed CVE’s on the MITRE site: <https://cve.mitre.org/cve/search_cve_list.html> | < > |
| **Third-party Applications & Patching** | | |
| **V**  **W** | What is your 3rd party patching policy/procedure? (This includes Adobe, browser plugins, etc.) | < > |
| How often are 3rd party patches applied? | < > |
| **V**  **W** | How do you test patches/updates for malicious code before the patches/updates are deployed to UNMH/Vendor systems? | < > |
| **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 < > Explain |
| **R** | Please specify Department or IT unit responsible for 3rd party patching? | < > |
| **Incident Response Components** | | |
| **V**  **W** | Which organization is the primary interface for security incidents, or other incidents to the system? | < > |
| **V**  **W** | When an incident involving UNMH EPHI data is detected, when is UNMH Notified? Frequency of IR Notifications? | < > |
| **V**  **W** | All SAAS vendors must provide UNMH a SAS70 ISO 270001 report related to their implementation/deployment of their security controls related to their organization and their IAAS/PAAS vendor (s) (Listing of their policies/procedures)  Can you supply this report? | < > |
| **V**  **W** | ALL SAAS vendors must supply or provide a risk-disclosure of their SAAS cloud locations-any IAAS/PAAS facilities outside of US locations or usage | < > |
| **V**  **W** | Do you Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity? | Yes  No < > Explain |
| **V**  **W** | Do you establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities? | Yes  No < > Explain |
| **V**  **W** | Do you Provide audit record reduction and report generation to support on-demand analysis and reporting? | Yes  No < > Explain |
| **V**  **W** | Do you track, document, and report incidents to designated officials and/or authorities both internal and external to the organization. | Yes  No < > Explain |
| **V**  **W** | Do you protect audit information and audit logging tools from unauthorized access, modification, and deletion?  Do you limit management of audit logging functionality to a subset of privileged users? | Yes  No < > Explain |
| **Disaster Recovery Process/Options** | | |
| **R** | What are the Disaster Recovery plans/processes failover and backup services for this system? | < > |
| **V**  **W** | What is the Vendor’s DR plan for their SAAS application in a 3rd party IAAS/PAAS location, what is the 3rd party IAAS/PAAS DR plan.  The SAAS vendor must provide evidence related to how they provide Disaster Recovery (DR) for our data/access to their software. | < > |
| **V**  **W** | SAAS vendor must determine and document what DR rate/priority they rank UNMH at in order to get our systems back up in the event of a DR incident. | < > |
| **Physical Security** | | |
| **R** | Are there any special physical security requirements (cameras, key-card access to system, etc.)? | < > |
| **Outsourcing Requirements** | | |
| **V**  **W** | 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** | | |
| **V** | Do ICD-10 or 5010 Transaction Standards apply? | < > |
| **Security Training** | | |
| **V**  **W** | Who is responsible for providing training for this system? | < > |
| **V**  **W** | Do you ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems? | Yes  No |
| **V**  **W** | Do you ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities? | Yes  No |

**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.**

**Note 2: When the ePHI data fields used, the impact is medium (2) if it ”will not result in loss of ePHI or PII in excess of 500 record** **and the impact is high if it “may result in loss of ePHI or PII in excess of 500 records”. If the likelihood is low (1) or medium (2).**

**Medium impact (2) × Medium Likelihood (2) = (4) Medium Risk. Review the Likelihood ratings related to vulnerabilities found and Mitigations that can be used to reduce the likelihood and Impact.**

**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) Vulnerability/Mitigation Score=**

**2) Impact versus Likelihood Score=**

**3) Internet-Facing Exploit Risk=** YesNo

**4) Vendor Soc2/SSAE16 Submitted for Vendor Assumed Risk:** YesNo

**5) Qualys SSL Labs Vendor Web Site Rating/Score=**

**6) Data Classification:**

* **Responsible Party for EPHI Data Security (Level 1):** VendorHealth SystemsBoth
  + **If EPHI & PII Data Used, How Many Records:** <500 Records>500Records
* **Restricted Data Security (Level 2):** VendorHealth SystemsBoth
* **Unrestricted (Public) Data (Level 3):** VendorHealth SystemsBoth

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

**Security Review Date:** < >

**Security Manager Name:** < >

**Security Manager Summary:** < >

**Security Review Date:** < >