

# Memorial Healthcare System

## ENTERPRISE SYSTEM ACCESS REQUEST FORM

You have the right to not provide the personal information on this form. If you choose not to complete this form in its entirety, you will be required to present yourself in person to the Department leader/MHS sponsor approving the access so that we can confirm your identity.

**Please fill out this form entirely. Incomplete forms can delay your account setup process.**  
**NON-MHS EMPLOYEES: ALL REQUIRED NOTICES MUST BE SENT TO MHS IT SYSTEM ACCESS TEAM VIA FAX (954-276-5397) OR EMAIL (MHSAccessRequestformONLY@mhs.net)**  
**MHS EMPLOYEES: PLEASE SUBMIT AN ONLINE REQUEST AND ATTACH COMPLETED FORM**

**\*\*All Users are required to read the following Policies. Initial by each Policy to confirm that you have received it.**

- **System Access Establishment, Modification and Termination Policy and Procedure** \_\_\_\_\_
- **Risk Analysis and Risk Management Policy** \_\_\_\_\_
- **Information System Activity Review Policy and Procedure** \_\_\_\_\_

USER INFORMATION (TO BE FILLED OUT BY THE PERSON REQUIRING ACCESS)				
*Today's Date:	* Legal Last Name:	*Legal First Name:	MI:	
Note: As part of the user ID creation process, all users will automatically be setup with MHS network login IDs as well as an MHS email account (if requested). User IDs are normally established with the first initial of the first name and complete last name, depending on availability. Please write legibly. You will be notified by MHS when the user ID is established. If an MHS email account is set up, we will use the email address to send periodic updates and other important system-related notifications, so please be sure to check this email account often.				
*Birth Date (MM/DD/YY):	*Office Phone:	* Last 4 digits Social Security #:		
*Office street address:			*Mobile Phone:	
*City:	*State:	*Zip Code:	* Your Email Address:	
The above information is true to the best of my knowledge. I understand my obligations under MHS policies and applicable law, including <b>HIPAA</b> and related rules and regulations, and agree to utilize information only as needed to perform my job as part of the workforce of a Covered Entity or as a Business Associate of a Covered Entity (each as defined in HIPAA). <b>I agree to comply with all MHS policies and procedures, and the terms of the Confidentiality and Data Security Agreement attached to this 3 page form and incorporated by reference. I agree that I am responsible for maintaining the custody and security of any MHS data I access, view, print, download or otherwise obtain from MHS. It is my sole responsibility to report any suspected breach of security or loss of custody of any MHS confidential information to the Privacy Reporting Number (954) 265-1165 or I can also send an email to mhsprivacy@mhs.net.</b>				
*Requestor's Signature:			*Date:	
MHS SPONSOR VERIFICATION SECTION (TO BE FILLED OUT BY MHS SPONSOR ONLY FOR CONTRACTOR/STUDENT/VENDOR REQUESTS)				
User Title:		Company/School:		
Start Date:	End Date:	Sponsor's Employee ID #:		
Name of MHS Sponsor approving this request:				
Sponsor's Department:			Sponsor's Email Address:	
Sponsor's Title (Supervisor or above):			Sponsor's Office Phone:	
***Applications/Access Requested:				
The above information is true to the best of my knowledge. I understand my obligations under MHS policies and applicable law, including <b>HIPAA</b> and related rules and regulations, and certify that the above named user has a legitimate need to access MHS systems to perform duties for my department. I authorize this user to be setup with access to the systems as indicated on this form. I agree to notify MHS IT System Access Team via fax (954) 276-5397 or email <a href="mailto:MHSAccessRequestformONLY@mhs.net">MHSAccessRequestformONLY@mhs.net</a> of any changes to this user's status under my Department. All user IDs that are not used within a 3 month period will be disabled as a security precaution. I agree to comply with all MHS policies and procedures and will ensure that this user complies by those policies. Remote access to any MHS system may require the use of a type of security device such as a token. Upon termination of the user's assignment or duties in my department, I agree to immediately return all devices that have been provided to this user. I will immediately notify MHS IT System Access Team via fax (954) 276-5397 or email <a href="mailto:MHSAccessRequestformONLY@mhs.net">MHSAccessRequestformONLY@mhs.net</a> to delete the user IDs that have been setup for this user.				
Sponsor's Signature:			Date:	



**VENDOR/CONTRACTOR VERIFICATION SECTION**  
**(TO BE FILLED OUT BY VENDOR/CONTRACTOR LEADER APPROVING THIS REQUEST)**

**Name of Vendor/Contractor approving this request:**

**Name/Title of Person Signing for Contractor/Vendor#:**

**Office Phone:**

**Email Address:**

The above information is true to the best of my knowledge. I certify that the above named user is the agent or subcontractor of the above named vendor/contractor. Company authorizes this user to be setup with access to the systems as indicated on this form. Company will immediately notify MHS IT System Access Team via fax (954) 276-5397 or email [MHSAccessRequestformONLY@mhs.net](mailto:MHSAccessRequestformONLY@mhs.net) of any changes to this individual's status as the agent or subcontractor of the above named vendor/contractor such as extended leave or termination of employment or affiliation. All user IDs that are not used within a 3 month period will be disabled as a security precaution. Vendor/Contractor agrees to comply with all MHS policies and procedures and will ensure that this user complies by those policies. Upon termination of the user's employment or status agent or subcontractor, Company will immediately return all devices that have been provided to this user and will immediately notify MHS IT System Access Team via fax (954) 276-5397 or email [MHSAccessRequestformONLY@mhs.net](mailto:MHSAccessRequestformONLY@mhs.net) to delete the user access. **Vendor/Company agrees to hold harmless and indemnify MHS, its employees and agents from and against any and all claims damages, expenses and causes of action, including, without limitation, attorney fees at all levels, arising out of, related to, or by reason of any misconduct, negligence, or breach of the terms and conditions of this Enterprise Access Form.**

**Signature:**

**Date:**

**PHYSICIAN OFFICE STAFF VERIFICATION SECTION**  
**(TO BE FILLED OUT BY PHYSICIAN APPROVING THIS REQUEST)**

**Name of Physician approving this request:**

**Physician ID#:**

**Office Phone:**

**Email Address:**

The above information is true to the best of my knowledge. I understand my obligations as a Covered Entity under MHS policies and applicable law, including HIPAA and related rules and regulations, and certify that the above named user is part of my workforce. I authorize this user to be setup with access to the systems as indicated on this form. I agree to immediately notify MHS of any changes to this individual's status as part of my workforce such as extended leave or termination of employment. All user IDs that are not used within a 3 month period will be disabled as a security precaution. I agree to comply with all MHS policies and procedures and will ensure that this user complies by those policies. Remote access to any MHS system may require the use of a type of security device such as a token. Upon termination of the user's employment or status as part of my workforce, I agree to immediately return all devices that have been provided to this user and will immediately notify MHS IT System Access Team via fax (954) 276-5397 or email [MHSAccessRequestformONLY@mhs.net](mailto:MHSAccessRequestformONLY@mhs.net) to delete the user IDs that have been setup for this user.

**\*\*\*Physician Signature:**

**Date:**

**\*\*\* All Physicians are required to comply with applicable law and MHS System policies, including but not limited to the MHS HIPAA Compliance Program, regarding access, use, and disclosure of medical information. Physicians who fail to comply with MHS policies shall be subject to corrective action.**

All information gathered on this form is confidential in accordance with applicable law, as part of the MHS Security Program and is only used to verify identity. All requests will be logged via the MHS Service Now ticketing system for record keeping purposes. If you have any questions about this form please call 954-276-4848 (MHS IT Service desk).

**MEMORIAL HEALTHCARE SYSTEM**

Memorial Regional Hospital  
Memorial Hospital Pembroke  
Memorial Manor

Joe DiMaggio Children's Hospital  
Memorial Hospital Miramar  
Memorial Home Health

Memorial Hospital West  
Memorial Regional Hospital South

**CONFIDENTIALITY AND DATA SECURITY AGREEMENT**

Patient Care Services provided by the Memorial Healthcare System (further referred to as Healthcare System or MHS) for its patients are privileged and confidential under the law, as is other information used by the Healthcare System in its operations. Other confidential and privileged information includes, without limitation, medical review/peer review committee information, risk management information, quality improvement information, and trade secrets. I will not make any illegal copies of material subject to the copyright laws. To enable the Healthcare System to perform those services, patients furnish information with the understanding that it will be kept confidential and used only by authorized persons as necessary in providing those services. The goodwill of the Healthcare System depends upon keeping such services and information confidential, that certain legal obligations attach to this information, and that by reason of your duties you may receive or have access to verbal, written or electronic media information concerning patients and services performed by the Healthcare System. **If you have any questions, please ask for clarification.**

Where there is any question as to the privileged or confidential nature of any information, or the right of any party to obtain information, the Healthcare System attorney should be consulted.  
RL 14244



**YOUR SIGNATURE ON PAGE THREE INDICATES ACCEPTANCE OF THE FOLLOWING:**

User agrees to hold harmless and indemnify MHS, its employees and agents from and against any and all claims damages, expenses and causes of action, including, without limitation, attorney fees at all levels, arising out of, related to, or by reason of any misconduct, negligence, or breach of the terms and conditions of this Enterprise Access Form.

- 1) **I HEREBY AGREE, I WILL NOT ACCESS ANY COMPUTER OR ELECTRONIC DATA, EXCEPT AS REQUIRED TO PERFORM MY DUTIES AND SUBJECT TO THE ABOVE LIMITATIONS.** I further agree that, except as directed by the Healthcare System or as required by law, I will not at any time disclose or misuse any confidential or privileged information to any unauthorized person, or permit any such person to examine or make copies of any reports or other documents prepared by me, coming into my possession or control, or to which I have access, that concerns in any way the privileged or confidential information of the Healthcare System.
- 2) **Work Station Security:** Under no circumstances will I give my password to any other individual. I will choose quality passwords, which I will remember. I will not write my password where another individual may find it. I will log out or secure my workstation whenever I leave the workstation, including closing blinds and placing patient identifiable information in a secure area out of plain view. I will not use a workstation that has been logged onto by another user unless I log them out. All information gained by my password will be treated as confidential and never be released to any person or misused unless they have a need to know and I have been authorized to release that information by my supervisor. I understand that I will be held responsible for all computer transactions that occur under my sign-on. I understand that all data from, or on MHS computers and computer systems is legally owned by the Healthcare System. I will not electronically copy or transmit MHS information (patient, financial, etc.) not directly related to my authorized duties without written consent from the authorized source. I understand the need to protect the Healthcare System's assets (its data), and that every individual is responsible for data security. I will report any and all suspected security breaches to the Chief Information Security Officer / Corporate Directory of Privacy. I can also call the Privacy Reporting Number (954) 265-1165 or email mhsprivacy@mhs.net. I understand that if I have been given remote access to the Healthcare System's computer system, I will abide by all of the above conditions.



**I RECOGNIZE THAT THE UNAUTHORIZED ACCESS AND/OR DISCLOSURE OF INFORMATION BY ME MAY VIOLATE STATE OR FEDERAL LAWS, AND THAT THE UNAUTHORIZED ACCESS AND/OR RELEASE OF INFORMATION MAY RESULT IN CRIMINAL AND/OR CIVIL LIABILITY, DISMISSAL OR OTHER DISCIPLINARY ACTION BEING TAKEN AGAINST ME.**

- 3) **Security of Healthcare System Information/Equipment:** I agree that I will comply with all security regulations in effect at the Healthcare System. I understand that all software used on a computer owned by the Healthcare System must be properly licensed and approved by the Healthcare System Administration for use on that computer. The use of unlicensed or unapproved software constitutes a serious risk to Healthcare System operations. If I use or allow to be used any unlicensed or unapproved software on a Healthcare System computer, I may be subject to criminal and/or civil liability, dismissal or other disciplinary action. **I acknowledge that an IT Security presentation is available on the MHS intranet site under IT Security, under the section marked, IT Security Presentations. I agree to access and completely review this presentation prior to any other use of MHS computer systems.**

Print Requestor's Full Name: \_\_\_\_\_

Requestor's Signature: \_\_\_\_\_ Date: \_\_\_\_\_



 <b>Memorial</b> Healthcare System	<i>Policy and Procedure</i>	<i>INFORMATION TECHNOLOGY: IT Security</i>	POLICY NUMBER: <i>IT-SEC-18</i>
<b>Policy Name: System Access Establishment, Modification and Termination Policy and Procedure</b>			
<b>Date Created: September 2017</b>		<b>Date Last Reviewed: October 2017</b>	
<b>Approved:</b> 		<b>Date of CIO Signature: 11/01/2017</b>	

## PURPOSE

The purpose of this policy is to implement procedures for establishing, modifying, and terminating access to systems, including electronic Protected Health Information (ePHI), as each person's job function(s) begins, changes, or ends.

## SCOPE

This policy applies to all MHS workforce members, business associates, vendors, affiliated physicians, and their practices and their employees.

## POLICY

Memorial Healthcare System recognizes the importance of appropriate access to systems, and particularly the importance of protecting our assets from unauthorized personnel.

In compliance with applicable laws and regulations, including HIPAA and other state and federal privacy laws, MHS has established procedures for (i) initial access for new workforce members, business associates, contractors, vendors, affiliated physicians, and their practices and their employees, (ii) modification of access for job function changes, and (iii) termination of access following employment termination or end of business function requiring access.

## PROCEDURE

### 1. Employees

#### a. **Employee Provisioning**

The Employee provisioning process begins when a new employee is added to the Human Resources Information System (HRIS). The HRIS sends a trigger file, which is a set of input parameters utilized for provisioning, containing the necessary information for the new employee to the provisioning system.



When the the provisioning system receives the trigger file from the HRIS, access to applications is automatically granted based on the role that is assigned to the user. The roles are defined based on three criteria:

1. Location
2. Department
3. Job code

Role-based automatic access is **ONLY** granted to those applications managed by the provisioning system that are appropriate for the job code at that specific location / department.

For those applications that are not part of the automated provisioning process, the user / manager submits a request via our Service Management system. The System Access Team will only grant this additional access if approved by manager/ lead.

Owner/Author:	<b>This document is controlled by Information Technology</b>	1  Status: Final
HIPAA Security Rule CFR#	<b>164.308(a)(3)(ii)(C) and 164.308(a)(4)(ii)(C)</b>	

 <b>Memorial</b> Healthcare System	<i>Policy and Procedure</i>	<i>INFORMATION TECHNOLOGY: IT Security</i>	<i>POLICY NUMBER: IT-SEC-18</i>
<b>Policy Name: System Access Establishment, Modification and Termination Policy and Procedure</b>			
<b>Date Created: September 2017</b>		<b>Date Last Reviewed: October 2017</b>	
<b>Approved:</b> 		<b>Date of CIO Signature: 11/01/2017</b>	

### **Employees accessing the MHS network / applications**

Employees receive their user name in the Core computer class when they start at MHS. They must reset their password via a System Access Team member in-class or call the MHS Service Desk for assistance.

### **b. Employee Transfers / Changes**

The Employee transfer / change process begins when an employee changes job function or transfers from one department / facility to another per the HRIS. A trigger file containing necessary information about the user is sent to the provisioning system.

When the the provisioning system receives the trigger file from the HRIS, the employee's access to applications is updated pursuant to the new role based on the below criteria. If the user has access to applications that are not part of the new role, the access to these applications will be automatically removed by the provisioning system.

The roles are defined based on three criteria:

1. Location
2. Department
3. Job code

### **c. Employee De-Provisioning**


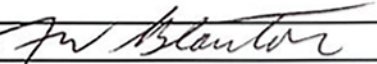
There are three (3) ways an employee's access can be terminated:

1. De-provisioning trigger file from the HRIS due to employee termination or resignation
2. Email from Human Resources or Legal/Privacy Department sent to the System Access Team for immediate access removal when necessary
3. Email from the Talent Acquisition Center (TAC) sent to the System Access Team if the user is classified as a DNS (does not start)

**The provisioning system will perform the following tasks for all three scenarios above:**

- a. Inactivate Active Directory (AD) account
- b. Disable password to prevent further access to data
- c. Email the 'IT Terminations' distribution list to notify application owners to check their application and process removal if necessary
- d. Remove all Active Directory groups
- e. Move Active Directory account to Disabled Accounts Organizational Unit (OU)
- f. Hide Mailbox
- g. Remove all applications listed in the provisioning System for the user

Owner/Author:	<b>This document is controlled by Information Technology</b>	2  Status: Final
HIPAA Security Rule CFR#	<b>164.308(a)(3)(ii)(C) and 164.308(a)(4)(ii)(C)</b>	

 <b>Memorial</b> Healthcare System	<i>Policy and Procedure</i>	<i>INFORMATION TECHNOLOGY: IT Security</i>	POLICY NUMBER: <i>IT-SEC-18</i>
<b>Policy Name: System Access Establishment, Modification and Termination Policy and Procedure</b>			
<b>Date Created: September 2017</b>		<b>Date Last Reviewed: October 2017</b>	
<b>Approved:</b> 		<b>Date of CIO Signature: 11/01/2017</b>	

- h. Generate a request in our Service Management system to process the remaining applications not in the provisioning system

## 2. **Non-Employees**

### a. **Non-Employee Provisioning**

For business associates, contractors, vendors, students, and physicians accessing MHS systems who are not part of MHS Medical Staff, a MHS sponsor submits an On-Boarding form via our Service Management system with an attached Enterprise System Access Request Form.

For affiliated physicians' practices and their employees, the Office Site Manager submits the Enterprise System Access Request Form (ESARF) for each user that requires access to EpicLink. ESARF issued after the date of this Policy's effective date shall include a certification that the physician and the physician's office staff have read and will comply with MHS privacy and security policies.

Access to necessary applications listed below are automatically granted based on the role that is assigned to the user. The roles are defined based on these criteria:

1. Non-employee's type
2. Non-employee's subtype

Role-based automatic access is ONLY granted to those applications managed by the provisioning system that are appropriate for the user's corresponding role.

For those applications that are not part of the automated provisioning process, the MHS sponsor/non-employee submits a request via the MHS Service Management system. The System Access Team will grant this additional access if approved by the MHS sponsor.

#### **Non-employees accessing the MHS network / applications**

Non-employee calls the MHS Service Desk and, after confirmation of the individual's identity, the MHS Service Desk provides the user ID and temporary password. The non-employee is required to change the temporary password upon the initial log-in.

### b. **Non-Employee De-Provisioning**


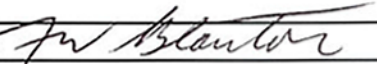
There are three (3) ways a non-employee's access can be terminated:

#### 1. **Monthly Site Verification process (specific to Epic / EpicLink users)**

Monthly Site Verification is a function in Epic / EpicLink that allows the Sponsor of Office Site Manager to validate the Epic/EpicLink access for all users. Site Verification is utilized for the purpose of reviewing the termination of Epic/EpicLink access for the staff who have left the group / practice.

Owner/Author:	<b>This document is controlled by Information Technology</b>	3
HIPAA Security Rule CFR#	<b>164.308(a)(3)(ii)(C) and 164.308(a)(4)(ii)(C)</b>	Status: Final



 <b>Memorial</b> Healthcare System	<i>Policy and Procedure</i>	<i>INFORMATION TECHNOLOGY: IT Security</i>	<i>POLICY NUMBER: IT-SEC-18</i>
<b>Policy Name: System Access Establishment, Modification and Termination Policy and Procedure</b>			
<b>Date Created: September 2017</b>		<b>Date Last Reviewed: October 2017</b>	
<b>Approved:</b> 		<b>Date of CIO Signature: 11/01/2017</b>	

- a. On the first day of the month, all offices/groups that did not complete the Monthly Site Verification for previous month are identified.
- b. Users identified are inactivated in Epic / EpicLink.
- c. If the user no longer needs access to Epic / EpicLink, the System Access Team terminates the user's account via the provisioning system.

## 2. **Expiration Date**

If an expiration date is set in the non-employee Active Directory account:

- a. 14 days prior to the account expiring, the sponsor will receive an email notifying them their sponsored user's account will be expiring
- b. If access has not been extended by 7 days prior to expiration date, the sponsor will receive another email notifying them their sponsored user's account will be expiring
- c. If access has not been extended by the expiration date, the sponsor will receive a final email notifying them their sponsored user's account has expired and the removal of all applications has been initiated by the provisioning system.

## 3. **Requests submitted via our Service Management system**

MHS Sponsor will submit a request for the non-employee's access termination via our Service Management system. System Access Team will process a full access termination via the provisioning system.

**The provisioning system will perform the following tasks for scenarios 2 and 3 above:**


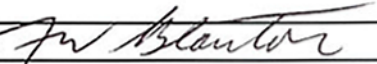
- a. Inactivate Active Directory account
- b. Disable password to prevent further access to data
- c. Email 'IT Terminations' distribution list to notify application owners to check their application and process removal if necessary
- d. Remove all Active Directory groups
- e. Move to Disabled Accounts Organizational Unit (OU)
- f. Hide Mailbox
- g. Remove all applications listed in the provisioning system for the user
- h. Generate a request in our Service Management system to process the remainder applications not in Provision

## 3. **MHS Hospitals' Medical Staff**

### a. **MHS Hospitals' Medical Staff Provisioning**

The MHS Hospitals' Medical Staff provisioning process begins when the monthly Board report showing medical staff credentialing activity is approved and sent to the System Access Team.

Owner/Author:	<b>This document is controlled by Information Technology</b>	4
		Status: Final
HIPAA Security Rule CFR#	<b>164.308(a)(3)(ii)(C) and 164.308(a)(4)(ii)(C)</b>	

 <b>Memorial</b> Healthcare System	<i>Policy and Procedure</i>	<i>INFORMATION TECHNOLOGY: IT Security</i>	POLICY NUMBER: <i>IT-SEC-18</i>
<b>Policy Name: System Access Establishment, Modification and Termination Policy and Procedure</b>			
<b>Date Created: September 2017</b>		<b>Date Last Reviewed: October 2017</b>	
<b>Approved:</b> 		<b>Date of CIO Signature: 11/01/2017</b>	

The System Access Team uses the Board report to manually create trigger files containing the necessary information for each user.

When the trigger file for MHS Hospitals' Medical Staff is received by the provisioning system, access to applications is automatically granted based on the role that is assigned to the user.

The roles are defined based on Specialty.

Role-based automatic access is ONLY granted to those applications managed by the provisioning system that are applicable for that Specialty.

For those applications that are not part of the automated provisioning process, MHS Hospitals' Medical Staff submits a request via our Service Management system. The System Access Team will grant this additional access if applicable.

#### **MHS Hospitals' Medical Staff accessing the MHS network / applications**

MHS Hospitals' Medical Staff calls the MHS Service Desk and, after confirmation of the individual's identity, the MHS Service Desk provides the user ID and temporary password. The Medical Staff is required to change the temporary password upon the initial log-in.

#### **b. MHS Hospitals' Medical Staff De-Provisioning**

The MHS Hospitals' Medical Staff de-provisioning process begins when the monthly Board report is approved and sent to the System Access Team or via an email directing deprovisioning from Human Resources, Legal/Privacy, or the MHS Chief Medical Officer.


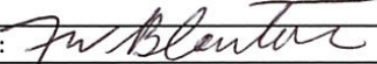
The System Access Team uses the Board report to manually create de-provisioning trigger files containing the necessary information for each Medical Staff member who is no longer with MHS.

#### **The provisioning system will perform the following tasks:**

- a. Inactivate Active Directory account
- b. Disable password to prevent further access to data
- c. Email 'IT Terminations' distribution list to notify application owners to check their application and process removal if necessary
- d. Remove all Active Directory groups
- e. Move Active Directory account to Disabled Accounts Organizational Unit (OU)
- f. Hide Mailbox
- g. Remove all applications listed in the provisioning system for the user
- h. Generate a request in our Service Management system to process the remainder applications not in the provisioning system

Owner/Author:	<b>This document is controlled by Information Technology</b>	5  Status: Final
HIPAA Security Rule CFR#	<b>164.308(a)(3)(ii)(C) and 164.308(a)(4)(ii)(C)</b>	



 <b>Memorial Healthcare System</b>	<b>Policy and Procedure</b>	<b>INFORMATION TECHNOLOGY: IT Security</b>	<b>POLICY NUMBER: IT-SEC-16</b>
<b>Policy Name: HIPAA Risk Analysis and HIPAA Risk Management Policy</b>			
<b>Date Created: September 2017</b>		<b>Date Last Reviewed: October 2017</b>	
<b>Approved:</b> 		<b>Date of CIO Signature: 11/01/2017</b>	

## Purpose:

This policy defines how Memorial Healthcare System (MHS) manages risks that can affect the availability, confidentiality, and integrity of its electronic Protected Health Information (ePHI) and assets containing ePHI in compliance with applicable state and federal laws and regulations.

## Scope:

MHS shall utilize the risk management approaches stated within this policy to identify and assess vulnerabilities, threats, and mitigating controls to all electronic Information Systems containing ePHI, all electronic media containing ePHI, and all ePHI created, stored, processed or transmitted by MHS.

## Policy:

MHS assesses all Information Systems and electronic media for risks that threaten the integrity, availability, and confidentiality of MHS ePHI and assets containing ePHI.

## Responsibility

The Chief Information Officer (CIO) or his designee is responsible for determining that this policy remains operationally fit for its purpose, is appropriately communicated to MHS workforce members, and documented.

## HIPAA Risk Analysis

The HIPAA risk analysis process is used as the basis for the identification, definition, and prioritization of risks. MHS revisits and adapts the HIPAA risk analysis process as environmental, operational, and technical changes arise. The HIPAA risk analysis process includes the following:


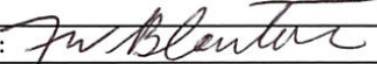
- Identification and prioritization of threats to ePHI and other information resources;
- Identification and prioritization of vulnerabilities to ePHI and other information resources;
- Identification of a threat that may exploit a vulnerability;
- Identification of measures and/or controls used to protect the confidentiality, integrity, and availability of ePHI and other information resources.

## Scoring Methodology

The tables below outline the framework that MHS' Information Security department uses to assess and prioritize risks identified during the HIPAA risk analysis and to evaluate their potential consequences to the organization. The risk calculation focuses specifically on the likelihood of a risk occurring given the internal controls in place at MHS, as well as the impact that an occurrence would have on MHS' patients, operations, ePHI, and assets. Each risk area should be assigned a level of likelihood and impact, based on the definitions below in Tables 1 and 2.

**Table 1: Likelihood of Threat Initiation, Occurrence, and Result of Adverse Impacts**

Owner/Author: IT Security	<b>This document is controlled by Information Technology</b>	1
HIPAA Security Rule CFR#	<b>164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(ii)(D), 164.308(a)(8),</b>	Status: Final


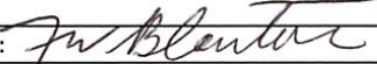
 <b>Memorial Healthcare System</b>	<b>Policy and Procedure</b>	<b>INFORMATION TECHNOLOGY: IT Security</b>	<b>POLICY NUMBER: IT-SEC-16</b>
<b>Policy Name: HIPAA Risk Analysis and HIPAA Risk Management Policy</b>			
<b>Date Created: September 2017</b>		<b>Date Last Reviewed: October 2017</b>	
<b>Approved:</b> 		<b>Date of CIO Signature: 11/01/2017</b>	

<b>Likelihood Level</b>	<b>Description</b>
<b>Very High</b> ●	<ul style="list-style-type: none"> <li>Adversary<sup>1</sup> is <b>almost certain</b> to initiate the threat event; <b>or</b> the error, accident; or act of nature is almost certain to occur; or occurs more than 100 times a year; <b>and</b></li> <li>If the threat event is initiated or occurs, it is <b>almost certain</b> to have adverse impacts.</li> </ul>
<b>High</b> ●	<ul style="list-style-type: none"> <li>Adversary is <b>highly likely</b> to initiate the threat event; <b>or</b> the error, accident, or act of nature is highly likely to occur; or occurs between 10-100 times a year; <b>and</b></li> <li>If the threat event is initiated or occurs, it is <b>highly likely</b> to have adverse impacts.</li> </ul>
<b>Moderate</b> ●	<ul style="list-style-type: none"> <li>Adversary is <b>somewhat likely</b> to initiate the treat event; <b>or</b> the error, accident, or act of nature is somewhat likely to occur; or occurs between 1-10 times a year; <b>and</b></li> <li>If the threat event is initiated or occurs, it is <b>somewhat likely</b> to have adverse impacts.</li> </ul>
<b>Low</b> ●	<ul style="list-style-type: none"> <li>Adversary is <b>unlikely</b> to initiate the threat event; <b>or</b> the error, accident, or act of nature is unlikely to occur; or occurs less than once a year, but more than once every 10 years; <b>and</b></li> <li>If the threat event is initiated or occurs, it is <b>unlikely</b> to have adverse impacts.</li> </ul>
<b>Very Low</b> ●	<ul style="list-style-type: none"> <li>Adversary is <b>highly unlikely</b> to initiate the threat event; <b>or</b> error, accident, or act of nature is highly unlikely to occur; or occurs less than once every 10 years; <b>and</b></li> <li>If the threat event is initiated or occurs, it is <b>highly unlikely</b> to have adverse impacts.</li> </ul>

<b>Table 2: Impact of Threat Events</b>	
<b>Impact Level</b>	<b>Description</b>
<b>Very High</b> ●	The threat event could be expected to have <b>multiple severe or catastrophic</b> adverse effects on organizational operations, organizational ePHI and assets containing ePHI, patients, or other organizations, or the local community.
<b>High</b> ●	<p>The threat event could be expected to have a <b>severe or catastrophic</b> adverse effect on organizational operations, organizational ePHI and assets containing ePHI, patients, other organizations, or the local community. A severe or catastrophic adverse effect means that, for example, the threat event might:</p> <ul style="list-style-type: none"> <li>(i) Cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;</li> <li>(ii) Result in major damage to organizational assets;</li> <li>(iii) Result in major financial loss; or</li> <li>(iv) Result in severe or catastrophic harm to patients involving loss of life or serious life-threatening injuries.</li> </ul>
<b>Moderate</b> ●	<p>The threat event could be expected to have a <b>serious</b> adverse effect on organizational operations, organizational ePHI and assets containing ePHI, patients other organizations, or the local community. A serious adverse effect means that, for example, the threat event might:</p> <ul style="list-style-type: none"> <li>(i) Cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;</li> <li>(ii) Result in significant damage to organizational assets;</li> <li>(iii) Result in significant financial loss; or</li> <li>(iv) Result in significant harm to patients that does not involve loss of life or serious life-threatening injuries.</li> </ul>

<sup>1</sup> The NIST *Guide for Conducting Risk Assessments* defines “adversary” as an Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.

Owner/Author:	<b>This document is controlled by Information Technology</b>	2
HIPAA Security Rule CFR#	<b>164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(ii)(D), 164.308(a)(8),</b>	Status: Final

 <b>Memorial Healthcare System</b>	<b>Policy and Procedure</b>	<b>INFORMATION TECHNOLOGY: IT Security</b>	<b>POLICY NUMBER: IT-SEC-16</b>
<b>Policy Name: HIPAA Risk Analysis and HIPAA Risk Management Policy</b>			
<b>Date Created: September 2017</b>		<b>Date Last Reviewed: October 2017</b>	
<b>Approved:</b> 		<b>Date of CIO Signature: 11/01/2017</b>	

<b>Low</b> ●	The threat event could be expected to have a <b>limited</b> adverse effect on organizational operations, organizational ePHI and assets containing ePHI, patients other organizations, or the local community. A limited adverse effect means that, for example, the threat event might: (i) Cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) Result in minor damage to organizational assets; (iii) Result in minor financial loss; or (iv) Result in minor harm to patients.
<b>Very Low</b> ●	The threat event could be expected to have a <b>negligible</b> adverse effect on organizational operations, organizational ePHI and assets containing ePHI, patients other organizations, or the local community.


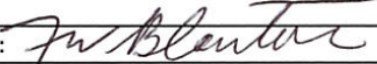
Once the risk is prioritized, an overall risk level should be assigned to each risk, based on the product of the likelihood and impact levels, as evidenced in Table 3. All risks are defined according to the descriptions in Table 4.

<b>Table 3: Risk Level Assessment Scale (Risk = Likelihood x Impact)</b>					
<b>Likelihood</b>	<b>Impact Level</b>				
	● <b>Very Low</b>	● <b>Low</b>	● <b>Moderate</b>	● <b>High</b>	● <b>Very High</b>
● <b>Very High</b>	Very Low	Low	Moderate	High	Very High
● <b>High</b>	Very Low	Low	Moderate	High	Very High
● <b>Moderate</b>	Very Low	Low	Moderate	Moderate	High
● <b>Low</b>	Very Low	Low	Low	Low	Moderate
● <b>Very Low</b>	Very Low	Very Low	Very Low	Low	Low

<b>Table 4: Risk Level Descriptions</b>	
● <b>Very High</b>	A threat event could be expected to have <b>multiple severe or multiple catastrophic</b> adverse effects on organizational operations, organizational ePHI, assets containing ePHI, patients, other organizations, or the local community.
● <b>High</b>	A threat event could be expected to have a <b>severe or catastrophic</b> adverse effect on organizational operations, organizational ePHI, assets containing ePHI, patients, other organizations, or the local community.
● <b>Moderate</b>	A threat event could be expected to have a <b>serious</b> adverse effect on organizational operations, organizational ePHI, assets containing ePHI, patients, other organizations, or the local community.
● <b>Low</b>	A threat event could be expected to have a <b>limited</b> adverse effect on organizational operations, organizational ePHI, assets containing ePHI, patients, other organizations, or the local community.
● <b>Very Low</b>	A threat event could be expected to have a <b>negligible</b> adverse effect on organizational operations, organizational ePHI, assets containing ePHI, patients, other organizations, or the local community.

Once the risk assessment process is completed and documented, the Information Security department will assign an "owner" of each identified risk (see below).

Owner/Author:	<b>This document is controlled by Information Technology</b>	3  Status: Final
HIPAA Security Rule CFR#	<b>164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(ii)(D), 164.308(a)(8),</b>	

 <b>Memorial Healthcare System</b>	<b>Policy and Procedure</b>	<b>INFORMATION TECHNOLOGY: IT Security</b>	<b>POLICY NUMBER: IT-SEC-16</b>
<b>Policy Name: HIPAA Risk Analysis and HIPAA Risk Management Policy</b>			
<b>Date Created: September 2017</b>		<b>Date Last Reviewed: October 2017</b>	
<b>Approved:</b> 		<b>Date of CIO Signature: 11/01/2017</b>	

### **Risk Mediation**

Remediation of risk is dependent on the classification of the risk.

Any recommendation to accept a risk will require approval from the CIO or Chief Information Security Officer (CISO). If a risk is accepted, the rationale for the acceptance must be documented by the Information Security department, which will evaluate and review the risk on a quarterly basis to determine if any further remediation is required. The results of the periodic risk evaluations will be documented.

### **Risk Owners**

Each risk will have an identified owner. The risk owner shall be the person with the authority to manage a risk. Risk owners may be the service owner, department head, or other individual responsible for the asset.

### **Risk Treatment Plans or Controls**

The IT Security team will work with risk owners in identifying possible risk treatment plans or controls to either eliminate or reduce the risk to an acceptable level. If a risk is not eliminated, either the CIO or CISO must provide their approval that a risk has been reduced to an "acceptable" level. The risk treatment plan or control shall be documented in the Information Service Management portal.

The appropriate security controls to eliminate or mitigate identified risks are selected by the Information Security department based on the nature, feasibility, and cost effectiveness of the controls.

### **Risk Monitoring**

The Information Security department will monitor the effectiveness of security measures designed to reduce risks and vulnerabilities to a reasonable and appropriate level. MHS processes to reduce risk to its ePHI and assets containing ePHI are as follows:


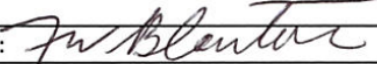
#### **I. Patch Management and Virus Protection**

1. All MHS Windows domain workstations and servers will be added to the monthly Operating System (OS) patch cycle process as outlined below:

The Information Security Department:

- a. Receives and reviews patch release information from Microsoft on the first Tuesday of each month;
  - b. Deploys patches the following Thursday to workstations at the Technology Resource Center;
  - c. Application/System owners monitor their respective applications to prevent adverse effect(s);
  - d. Deploys patches for all sites the following Monday unless alerted by an application/system owner of any issues.
2. All systems running a non-Windows OS are assessed quarterly for ongoing patching updates.
  3. Applications, such as Java and Adobe, are reviewed quarterly and patches will be applied if required.
  4. Anti-virus software is part of the base image. The anti-virus software will check daily for updates from the master repository.
  5. Application/system owners will coordinate monthly with their vendors for applying critical patches to Windows systems not managed by MHS.

Owner/Author:	<b>This document is controlled by Information Technology</b>	4
		Status: Final
HIPAA Security Rule CFR#	<b>164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(ii)(D), 164.308(a)(8),</b>	

 <b>Memorial Healthcare System</b>	<b>Policy and Procedure</b>	<b>INFORMATION TECHNOLOGY: IT Security</b>	<b>POLICY NUMBER: IT-SEC-16</b>
<b>Policy Name: HIPAA Risk Analysis and HIPAA Risk Management Policy</b>			
<b>Date Created: September 2017</b>		<b>Date Last Reviewed: October 2017</b>	
<b>Approved:</b> 		<b>Date of CIO Signature: 11/01/2017</b>	

## **II. Vulnerability Management**

1. All servers in the data center are scanned quarterly.
2. All new servers must be scanned before going into production.
3. Medical devices and non-MHS owned systems are scanned annually.
4. An internal vulnerability assessment will be performed by a third party every two years.
5. An external scan by a third party will be performed annually.
6. Vulnerabilities will be prioritized and remediated based on the severity.

## **III. System Monitoring**

1. MHS utilizes a Managed Security Service Provider to monitor, prevent, and alert on Probing, Denial of Service, or unauthorized access attempts from external sources.
2. A Network Access Control system is utilized to monitor and prevent unauthorized devices from connecting to the MHS internal network.
3. Access to critical systems that contain or process ePHI or confidential information are monitored or unauthorized access.
4. Removable media and email are monitored for the unsecure disclosure of confidential information.
5. MHS utilizes a Managed Privacy Provider for monitoring and alerting of privacy access violations. The Managed Privacy Provider analyzes and alerts MHS of any suspicious or potential malicious activity.

## **IV. Security Incident Response (Refer to MHS' Cyber Security Incident Response Plan)**

1. All security incidents shall be documented in the Information Service Management portal.
2. The Information Security department investigates all security incidents and determines the appropriate action to be taken based on severity.
3. The severity of the security incident will determine the escalation process as defined in the Cyber Security Incident Response Plan.

## **Risk Management Schedule**


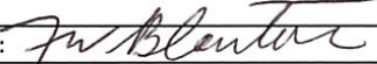
MHS' risk analysis and risk monitoring processes will be carried out according to the following schedule to determine the continued adequacy and improvement of the organization's Information Systems:

1. **Scheduled Basis** – an overall risk analysis of MHS' Information Systems will be conducted every two years. The analysis process should be completed in a timely fashion so that risk treatment plans or controls can be determined and included in the budgeting process.
2. **Throughout a System's Development Life Cycle** – from the time that a need for a new information system is identified through the time it is disposed of, ongoing assessments of the potential threats to a system and its vulnerabilities are undertaken as set forth in Section III, above.
3. **As Needed** – the MHS CIO or CISO may call for a full or partial risk analysis in response to changes in business strategies, information technology, information sensitivity, threats, legal liabilities, or other significant factors that affect MHS' Information Systems.

## **Documentation Requirements**

The MHS CISO or delegate documents or receives a copy of all documents pertaining to risk analyses and risk monitoring activities completed to comply with the HIPAA Security Rule, and maintains those documents for six years from the date of creation, or date it was last in effect, whichever is later.

Owner/Author:	<b>This document is controlled by Information Technology</b>	5
HIPAA Security Rule CFR#	<b>164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(ii)(D), 164.308(a)(8),</b>	Status: Final

 <b>Memorial Healthcare System</b>	<b>Policy and Procedure</b>	<b>INFORMATION TECHNOLOGY: IT Security</b>	<b>POLICY NUMBER: IT-SEC-16</b>
<b>Policy Name: HIPAA Risk Analysis and HIPAA Risk Management Policy</b>			
<b>Date Created: September 2017</b>		<b>Date Last Reviewed: October 2017</b>	
<b>Approved:</b> 		<b>Date of CIO Signature: 11/01/2017</b>	

**Supporting Documents**



- A. General Guidelines of MHS HIPAA Security Program
- B. Cyber Security Incident Response Plan
- C. Privacy Program Internal Reporting Procedure

**Legal Authority/References**

164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C),  
164.308(a)(6)(i), 164.308(a)(6)(ii), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.312(c)(1), 164.312(c)(2), 164.312(e)(2)(i)

Owner/Author:	This document is controlled by Information Technology	6  Status: Final
HIPAA Security Rule CFR#	164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(ii)(D), 164.308(a)(8),	



 <b>Memorial Healthcare System</b>	<b>Policy and Procedure</b>	<b>INFORMATION TECHNOLOGY: IT Security</b>	<b>POLICY NUMBER: IT-SEC-17</b>
<b>Policy Name: Information System Activity Review Policy and Procedure</b>			
<b>Date Created: September 2017</b>		<b>Date Last Reviewed: October 2017</b>	
<b>Approved:</b> 		<b>Date of CIO Signature: 11/01/2017</b>	

## PURPOSE

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule requires healthcare organizations to implement reasonable hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use electric Protected Health Information (ePHI). Memorial Healthcare System (MHS) is committed to safeguarding the confidentiality, integrity, and availability of patient health information applications, systems, and networks. MHS shall conduct system activity reviews to detect, report, and guard against network vulnerabilities and intrusions, breaches in the confidentiality and security of patient protected health information, and performance problems and flaws in applications that could impact the security and integrity of ePHI.


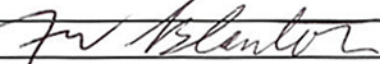
## SCOPE

This policy applies to all MHS workforce members, business associates, vendors affiliated physicians, and their practices and their employees.

## POLICY

1. Based on internal assessments of information security risk areas, MHS conducts regular reviews of information system activity, including the review of audit logs, access reports, and security incident tracking reports, for critical networks/systems/applications that contain ePHI. Review activities may be limited by application, system, and/or network reviewing capabilities and resources.
2. MHS collaborates with each critical network/system/application owner in order to determine which events are most likely to be correlated with risks to the confidentiality, integrity, and availability of the ePHI contained in the system and ensure that the content and level of detail included in system activity review are adequate.
3. All system activity reviews and incident reporting and response activities are conducted on a confidential, need-to-know basis.
4. Documentation produced as a result of system activity reviews (e.g., audit control reports, system/application logs, event logs, and any derivative reports generated from review activity) is kept and handled in a secure manner.
5. Workforce members responsible for system activity reviews shall immediately report any and all suspected breaches of information security and/or ePHI to MHS' Chief Information Security Officer.
6. All workforce members are trained regarding appropriate reporting of security incidents, as outlined in the Procedure for Internal Reporting.

Owner/Author: IT Security	<b>This document is controlled by Information Technology</b>	1  Status: Final
HIPAA Security Rule CFR#	<b>164.308(a)(1)(i), 164.308(a)(4)(i), 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(4)(ii)(C)</b>	

 <b>Memorial</b> Healthcare System	<b>Policy and Procedure</b>	<b>INFORMATION TECHNOLOGY: IT Security</b>	<b>POLICY NUMBER: IT-SEC-17</b>
<b>Policy Name: Information System Activity Review Policy and Procedure</b>			
<b>Date Created: September 2017</b>		<b>Date Last Reviewed: October 2017</b>	
<b>Approved:</b> 		<b>Date of CIO Signature: 11/01/2017</b>	



7. Periodic reports of summary results of systems activity reviews are presented to the Security and Privacy Committee.

## PROCEDURE

### A. Identification of Review Activities

1. MHS shall identify and document the systems, applications and networks that will be the focus of activity review efforts by:
  - a. Focusing efforts on areas of greatest risk and vulnerability as identified in the information systems risk analysis and ongoing risk management processes, historical organizational experience, current and projected future organizational needs, and industry trends and events.
  - b. Assessing the appropriate scope of activity reviews based on the size and needs of MHS by determining the:
    - i. Types of ePHI at risk;
    - ii. Processes that are vulnerable to unauthorized or inappropriate access, including those at the application, system and network levels;
    - iii. Activities that should be monitored; and
    - iv. Information to be included in the review record.
  - c. Assessing available organizational resources.
2. MHS shall identify and document circumstances which require ad hoc review activities using a risk-based approach through identification of anomalous system activity or criteria which raise awareness of questionable conditions regarding the viewing of ePHI. The system activity may be applied to the entire organization or may be specific to a department, unit, application or system.
  - a. At a minimum, MHS shall conduct a prompt review in response to:
    - i. A patient or employee complaint regarding his or her ePHI;
    - ii. A suspected breach incident involving ePHI;
    - iii. An identified high risk area or event; and
    - iv. A notification/external report involving MHS ePHI, such as from law enforcement.



Owner/Author:	<b>This document is controlled by Information Technology</b>	2  Status: Final
HIPAA Security Rule CFR#	<b>164.308(a)(1)(i), 164.308(a)(4)(i), 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(4)(ii)(C)</b>	

 <b>Memorial Healthcare System</b>	<b>Policy and Procedure</b>	<b>INFORMATION TECHNOLOGY: IT Security</b>	<b>POLICY NUMBER: IT-SEC-17</b>
<b>Policy Name: Information System Activity Review Policy and Procedure</b>			
<b>Date Created: September 2017</b>		<b>Date Last Reviewed: October 2017</b>	
<b>Approved:</b> 		<b>Date of CIO Signature: 11/01/2017</b>	

## **B. Conducting Review Activities**

1. The Chief Information Security Officer and/or the Corporate Director of Privacy shall designate the employees and/or contractors who are authorized to use information system activity review and monitoring tools. Such tools may not be used by anyone not specifically authorized. These tools may include, but are not limited to: vulnerability testing software, scanning tools and devices, intrusion detection systems, automated privacy monitoring software, and other tools as deemed necessary by MHS.
  - a. More than one person may be responsible for conducting the review functions for accountability purposes, but no more than necessary to perform the functions with respect to the size and complexity of the environment.
  - b. Workforce members may not conduct reviews that pertain to their own system activity unless there is no alternative or no inherent conflict of interest.
  - c. Workforce members performing review will have access to only the minimum resources necessary to perform his/her review duties.
  - d. Reviewers should have the appropriate technical skills with respect to the operating systems and applications necessary to access, interpret, and summarize the audit logs correctly.
2. MHS shall determine its ability to generate, review, and respond to review reports using its internal organizational resources. Where necessary, MHS may determine that the use of external resources is also appropriate for review activities.
3. Where possible, review documentation and/or reporting tools should address, at a minimum, the following data elements:
  - a. The application, system, network, department, and/or user reviewed;
  - b. The type of review conducted and the rationale for performing the review;
    - i. System activity review efforts may include a regular review of audit logs, access reports, and security incident tracking reports. The review should allow for a means to monitor information operations to determine if a specific incident occurred by providing a chronological series of logged computer events (e.g., review logs) that relate to an operating system, and application or user activities. Where possible, review processes may address the identification of the individual logging in/out; the date and time of each log-on attempt; date and time of each log-off attempt; devices used; the data accessed; the functions performed, for example: what did the user do - create, read, modify, deleted, add, etc; and other information, as necessary.

Owner/Author:	<b>This document is controlled by Information Technology</b>	3  Status: Final
HIPAA Security Rule CFR#	<b>164.308(a)(1)(i), 164.308(a)(4)(i), 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(4)(ii)(C)</b>	

 <b>Memorial Healthcare System</b>	<b>Policy and Procedure</b>	<b>INFORMATION TECHNOLOGY: IT Security</b>	<b>POLICY NUMBER: IT-SEC-17</b>
<b>Policy Name: Information System Activity Review Policy and Procedure</b>			
<b>Date Created: September 2017</b>		<b>Date Last Reviewed: October 2017</b>	
<b>Approved:</b> 		<b>Date of CIO Signature: 11/01/2017</b>	

- c. The individual and/or department responsible for conducting and approving the review;
- d. The date(s) the review was conducted;
- e. The information/data reviewed;
  - i. MHS IT Security will work with the appropriate system/application owner to ensure that an acceptable level of detail and content are included in activity logs, where used;
- f. The findings/conclusions from the review, including the determination of significant events requiring further review and follow-up; and
- g. Recommendations and/or follow up actions needed, based on review findings, including the identification of the appropriate reporting channels for review of results and required follow-up.



#### **C. Review Requests for Specific Cause**

1. The Chief Information Security Officer and/or Corporate Director of Privacy may receive requests to review information system activity for a specific cause. The request may come from a variety of sources including, but not limited to the following individuals/departments: an MHS patient, a MHS vendor or affiliate, Human Resources, Risk Management, Privacy, Legal, Information Technology and/or a member of MHS administration.
  - a. A request for a review for specific cause must include the time frame and nature of the request. The request must be reviewed and approved by the Chief Information Security Officer or the Corporate Director of Privacy, or his or her designee, prior to any action being taken.
  - b. A request for a review resulting from a patient concern shall be initiated by the Chief Information Security Officer and/or the Corporate Director of Privacy, or his or her designee. For incidents of a more sensitive nature, this individual shall consider the need to collaborate with Risk Management and/or Legal prior to communicating with the patient regarding review findings.

#### **D. Review and Reporting of Activity Review Findings**

1. Activities that are routinely gathered (e.g., system logs) must be reviewed in a timely manner.
2. Reporting the results of any review is limited to a minimum necessary/need to know basis. Review of results may be disclosed as deemed necessary. Legal should be consulted as needed.

Owner/Author:	<b>This document is controlled by Information Technology</b>	4  Status: Final
HIPAA Security Rule CFR#	<b>164.308(a)(1)(i), 164.308(a)(4)(i), 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(4)(ii)(C)</b>	

 <b>Memorial Healthcare System</b>	<b>Policy and Procedure</b>	<b>INFORMATION TECHNOLOGY: IT Security</b>	<b>POLICY NUMBER: IT-SEC-17</b>
<b>Policy Name: Information System Activity Review Policy and Procedure</b>			
<b>Date Created: September 2017</b>		<b>Date Last Reviewed: October 2017</b>	
<b>Approved:</b> 		<b>Date of CIO Signature: 11/01/2017</b>	

3. Information system review findings/results and reports gathered from contracted external review firms, business associates, and vendors shall be evaluated, and appropriate corrective action steps will be taken.
4. Suspected security incidents detected through activity review processes should be documented and immediately reported to the MHS Information Technology Department and/or the Chief Information Security Officer or his/her designee for follow-up.
5. The reporting process shall allow for meaningful communication of the review findings to the appropriate departments/units, as well as the Security and Privacy Committee. Significant findings shall be reported immediately. Routine findings shall be reported quarterly.
6. Activity reviews are a confidential monitoring practice and part of the organization's performance improvement activities and reporting. Results of these reviews should only be released to those individuals who are authorized to receive the information. Extreme caution should be taken when sharing review information that may further expose organizational risk.
7. Appropriate corrective actions indicated through review results must be undertaken accordingly. These actions shall be documented and shared with the responsible and sponsoring departments/units.
8. Criminal activity discovered during a review should be immediately reported to the General Counsel, the Chief Information Security Officer or his/her designee, the Corporate Director of Privacy or his/her designee, and law enforcement.



**E. Review of Business Associate and/or Vendor Access and Activity.**

1. Where necessary, the monitoring of business associate and vendor information system activity should be carried out to ensure that access and activity is appropriate for privileges granted, and necessary to the arrangement between MHS and the external agency.
2. If it is determined that the business associate or vendor has exceeded the scope of access privileges, MHS leadership must reassess the business relationship (refer to MHS business associate agreement/policy).
3. If it is determined that a business associate has violated the terms of the HIPAA business associate agreement, MHS must take immediate action to remediate the situation, up to and including termination of the business relationship.

**F. Integrity, Security and Backup of Activity Review Documentation.**

Owner/Author:	This document is controlled by Information Technology	5  Status: Final
HIPAA Security Rule CFR#	164.308(a)(1)(i), 164.308(a)(4)(i), 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(4)(ii)(C)	



 <b>Memorial Healthcare System</b>	<b>Policy and Procedure</b>	<b>INFORMATION TECHNOLOGY: IT Security</b>	<b>POLICY NUMBER: IT-SEC-17</b>
<b>Policy Name: Information System Activity Review Policy and Procedure</b>			
<b>Date Created: September 2017</b>		<b>Date Last Reviewed: October 2017</b>	
<b>Approved:</b> 		<b>Date of CIO Signature: 11/01/2017</b>	

1. The integrity of activity review documentation must be protected from unauthorized access or modification so that the information contained therein is available if needed.
2. Whenever possible, activity review information (i.e., audit trails) shall be stored on a separate system to prevent unauthorized access attempts and protect the information from malicious activity.
3. Review logs maintained within an application shall be backed-up as part of the application's regular backup procedures.

#### **G. Workforce Training, Education, Awareness and Responsibilities**

1. MHS workforce members shall receive training, education, and awareness on safeguarding the privacy and security of business and patient protected health information.
2. MHS' commitment to reviewing access and activity of the information applications, systems, and networks is communicated through new employee orientation, ongoing training opportunities and events, and access to applicable policies.
3. Workforce members are made aware of responsibilities with regard to privacy and security of information, including the applicable sanctions/corrective disciplinary actions, should the activity review process detect a workforce member's failure to comply with MHS policies.

#### **H. Retention of Review Records.**



1. Activity review documentation (for example, audit logs, access reports, and security incident tracking reports) shall be maintained based on organizational needs. Log data summarizing review activities shall be retained for a period of six (6) years.

#### **I. Policy Responsibility and Oversight.**

1. Responsibility for reviewing information system access and activity is assigned to the Chief Information Security Officer and/or the Corporate Director of Privacy and/or other designee as determined necessary. The responsible individual shall:
  - a. Assign the task of generating reports for review activities to the individual responsible for the application, system, or network.
  - b. Assign the task of reviewing the logs to the individual responsible for the application, system, or network, the Corporate Director of Privacy, or any other individual determined to be appropriate for the task.
  - c. Organize and provide oversight to a team structure charged with reviewing compliance activities (e.g., parameters, frequency, sample sizes, report formats, evaluation, follow-up, etc.).

Owner/Author:	<b>This document is controlled by Information Technology</b>	6  Status: Final
HIPAA Security Rule CFR#	<b>164.308(a)(1)(i), 164.308(a)(4)(i), 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(4)(ii)(C)</b>	



 <b>Memorial Healthcare System</b>	<b>Policy and Procedure</b>	<b>INFORMATION TECHNOLOGY: IT Security</b>	<b>POLICY NUMBER: IT-SEC-17</b>
<b>Policy Name: Information System Activity Review Policy and Procedure</b>			
<b>Date Created: September 2017</b>		<b>Date Last Reviewed: October 2017</b>	
<b>Approved:</b> 		<b>Date of CIO Signature: 11/01/2017</b>	

2. Periodic reports of summary results of systems activity reviews will be reported to the Security and Privacy Committee on a regular basis.



## DEFINITIONS

- **Business Associate:** A person or entity who, on the behalf of the covered entity, arranges, performs, or assists in certain functions, activities, or services involving the use or disclosure of protected health information. A business associate is not a member of the covered entity's workforce; however, a covered entity is permitted to be a business associate for another covered entity.
- **Health Insurance Portability and Accountability Act (HIPAA):** The Health Insurance Portability and Accountability Act of 1996 is codified at Title 45 of the U.S. Code of Federal Regulations (CFR), Part 160 and Subparts A and C of Part 164.
- **Electronic Protected Health Information (ePHI):** Protected health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.
- **Protected Health Information (PHI):** Any information, including demographic information collected from that individual, that (A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.
- **Security Rule:** The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. The Security Rule, promulgated by the U.S. Department of Health and Human Services (HHS) pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), is codified at Title 45 of the U.S. Code of Federal Regulations (CFR), Part 160 and Subparts A and C of Part 164. HHS published the Security Rule on February 20, 2003.
- **System Logs:** Records of activity maintained by the system which provide the data and time of activity, origin of activity, identification of user performing the activity and a description of the attempted or completed activity.

## RELATED DOCUMENTS

- A. Privacy Program Internal Reporting Policy

Owner/Author:	This document is controlled by Information Technology	7  Status: Final
HIPAA Security Rule CFR#	164.308(a)(1)(i), 164.308(a)(4)(i), 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(4)(ii)(C)	

 <b>Memorial</b> Healthcare System	<i>Policy and Procedure</i>	<i>INFORMATION TECHNOLOGY:</i> <b>IT Security</b>	POLICY NUMBER: <i>IT-SEC-17</i>
Policy Name: Information System Activity Review Policy and Procedure			
Date Created: September 2017		Date Last Reviewed: October 2017	
Approved: 		Date of CIO Signature: 11/01/2017	

**LEGAL AUTHORITY/REFERENCES**

164.308(a)(1)(ii)(D), 164.308(a)(5)(i), 164.308(a)(5)(ii)(A), 164.308(a)(5)(ii)(C), 164.308(a)(6)(i),  
164.308(a)(6)(ii),

Owner/Author:	This document is controlled by Information Technology	8
HIPAA Security Rule CFR#	164.308(a)(1)(i), 164.308(a)(4)(i), 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(4)(ii)(C)	Status: Final