HACKENSACK MERIDIAN *HEALTH*
OCEAN MEDICAL CENTER
GRADUATE MEDICAL EDUCATION
POLICIES AND PROCEDURES

Subject: BLOOD BORNE PATHOGENS	**Policy Number : 11.A**
Approved by GMEC: May 9, 2018	**Approved by MEC: June 7, 2018**

1. INTRODUCTION AND PURPOSE

   To establish guidelines in the event of exposure, or any incident that may place resident at risk, for all postgraduate trainees in all Residency programs sponsored by Meridian Hospitals Corporation (MHC)

2. SCOPE

   This policy will apply to all of the postgraduate training programs at MHC facilities.

3. APPLICABLE REGULATIONS AND GUIDELINES

   HMH Human Resources Policy **PolicyStat ID:** *4034345*

   Effective Date: July 1, 2018

Current Status: *Active*

PolicyStat ID: *4034345*

Origination Date:	*06/2015*
Last Approved:	*06/2017*
Last Revised:	*06/2017*
Next Review:	*06/2020*
Owner:	*Victoria Riveracruz: SR MGR TM & LABOR RELATIONS*
Policy Area:	*Human Resources - Occupational Health*
Applies To:	
Applicability:	*Legacy Meridian Health Group*

Hackensack Meridian *Health*

Blood Borne Pathogen Post Exposure (Needlestick or Mucous Membrane)

Purpose:

1. To protect a team member who sustains a parenteral, cutaneous, or mucous membrane exposure to a patient's blood and/or body fluids.
2. To ensure the appropriate treatment of all team members with direct exposure to a patient's blood and/or body fluids.

Scope:

All Meridian Health Team Members

Policy:

DEFINITIONS

Exposure is defined as any incident that may place a team member at risk for Hepatitis B virus (HBV), Hepatitis C virus (HCV), Human Immunodeficiency Virus (HIV) or Zika. The CDC defines the following as potential exposures:

a. Percutaneous exposure (e.g. needle stick or cut with sharp object) or mucous membrane exposure (e.g. splash to the eye or mouth) exposure of blood or other body fluid

b. Cutaneous exposure on non-intact skin (e.g. exposed skin that is chapped, abraded, or afflicted with dermatitis) with blood, tissue or other body fluids that are potentially infectious)

Risk of transmission of pathogen via blood, body fluids, secretions and excretions will be determined by the treting provider on a case basis.

Procedure:

Blood Borne Pathogen exposures are considered urgent medical concerns. It is imperative that timely post exposure management be instituted including administration of HBIG, if indicated, Hepatitis B vaccine and/or HIV Post exposure chemoprophylaxis.

Post exposure evaluation is available in Meridian Occupational Health during its hours of operation and in the

Emergency Department after hours to all team members who have had an occupational exposure.

If a team member is initially treated in the ED, follow up care is available in Occupational Health for all team members who have had an exposure.

The following steps outline immediate care for a post exposure incident:

1. If the exposure occurred to a mucous membrane, the team member should immediately flush the exposed mucous membrane with water.
2. If the exposure occurred to the skin surface or is a needle stick or puncture, the team member should immediately wash the exposed skin with soap and water.

All team members exposed to blood or other body fluids are required to:

1. Report the incident to his/her leader/supervisor immediately
2. Via Meridian Intranet access Meridian CareLink and complete a Team Member Incident report.
3. Via Meridian Intranet print the following forms: (Forms are available on the Meridian Intranet by going to "Printable Forms" and then to "Occupational Health forms".)
    a. Blood Borne Pathogen Post Exposure Checklist
    b. Blood Borne Exposure Attending Physician's Report of Source-Patient Risk Factors.
    c. Source BBP Lab Slip
4. Notify Source Patient's attending of incident and need for source screening and use telephone order to complete clinical risk assessment if attending not available for signature. Bring the completed form when presenting for treatment.
5. Leader/supervisor to review source's General Consent to verify source signed.
6. ONLY if source Consented: Complete "Source Lab Requisition" – make sure you indicate where the source rapid HIV screening is to be called to. Have specimens drawn and sent to lab with "Source Lab Requistion
7. If initial treatment done in ED call Occupational Health for follow up care.

Required data to be included in Meridian CareLink Team Member incident report :

1. Demographic data including job title and regular shift
2. Date and time of the exposure
3. Where the incident occurred – location within the facility
4. A description of the exposure incident including:
    a. Procedure/type of work performing at time of incident
    b. Cause of incident
    c. Objects or substances involved in incident
    d. What potentially infectious materials were involved
    e. Personal protective equipment being use at the time
    f. Identification of source
    g. Route(s) of exposure

h. Type and brand of sharp involved

Additional information that will be obtained by Occupational Health include:

1. If sharp had engineered sharps injury protection, whether the protective mechanism was activated, and whether the injury occurred before, during or after activation
2. If non-safety sharp used, your opinion as to whether and how such a mechanism could have prevented the injury
3. Your opinion about whether any other engineering, administrative or work practice control could have prevented the injury

Leaders/Supervisors are responsible to ensure the completion of all information as well as provide the exposed Team Member with directions for immediate care.

Source Patient

An extremely important part of blood borne pathogen exposure treatment is the evaluation of the source patient's Zika, HBV, HCV, and HIV status. The source patient's name, age, room, diagnosis, and attending physician are to be included on the incident report unless it is established by the Leader that source identification is not feasible.

The attending physician will be contacted by the unit leader where the source inpatient or outpatient is registered. The attending physician shall complete the "Attending Physician's Source-Patient Risk Factors" form and fax it to the appropriate Occupational Health office.

The following will be tested if the source patient signed the General Consent: Health Care Worker Exposure - Consent for Blood Testing:

HIV 1&2

Hepatitis B Antigen

Hepatitis C Antibody

Should the source patient's consent not be obtained and the source patient's blood will not be tested.

Results of the HIV 1&2 testing will be reported to the treating Occupational Health provider and/or the ED physician (to allow for determination of the appropriate chemoprophylaxis treatment needs of the HCP).

All laboratory studies will be charged to the Occupational Health Department.

Team Member will be notified by the ED/Occupational Health Provider of the determination of an exposure risk for possible transmission of Zika, HIV, Hepatitic C and/or Hepatitis B viruses.

All exposed team member shall have baseline and surveillance laboratory studies after receiving counseling and providing consent. Exposed HCP should be advised to use precautions to prevent secondary transmission post exposure during the surveillance period. (See Attachment: Guidelines for individuals following an Exposure to Blood & or Body Fluids).

No team member shall leave work wearing contaminated clothing.

If the team member consents to baseline blood collection, but does not give consent at that time for HIV serologic testing, the sample shall be preserved for at least 90 days. If within 90 days of the exposure incident, the team member elects to have the baseline sample tested, such testing shall be done as soon as feasible.

Pre-PolicyStat Number: MHS-ADMIN-01-1086

Attachments:

Blood Borne Pathogen Post Exposure Checklist
Bloodborne Pathogen Exposure Attending Physician's Report of Source-Patient Risk Factors
Guidelines for Individuals following an Exposure to Blood & or Body Fluids

Applicability

Bayshore Medical Center, Hackensack Meridian Health Inc. , Jersey Shore University Medical Center, Legacy Meridian Health, Ocean Medical Center, Raritan Bay Medical Center - Old Bridge Division, Raritan Bay Medical Center - Perth Amboy Division, Riverview Medical Center, Southern Ocean Medical Center

HACKENSACK MERIDIAN *HEALTH*
OCEAN MEDICAL CENTER
GRADUATE MEDICAL EDUCATION
POLICIES AND PROCEDURES

Subject: **EQUAL EMPLOYMENT OPPORTUNITY/ AFFIRMATIVE ACTION**	**Policy Number:** **11.B**
Approved by GMEC: May 9, 2018	**Approved by MEC: June 7, 2018**

Reference Human Resources Policies and Procedures Document #: **PolicyStat ID:** *3574066*

Effective July 1, 2018

Hackensack Meridian *Health*

Origination Date:	*12/2002*
Last Approved:	*01/2015*
Last Revised:	*01/2015*
Next Review:	*01/2018*
Owner:	*Victoria Riveracruz: SR MGR TM & LABOR RELATIONS*
Policy Area:	*Human Resources*
Applies To:	
Applicability:	*Legacy Meridian Health Group*

Equal Employment Opportunity/Affirmative Action

Purpose:

This policy will serve to reiterate that the team members and leadership of Meridian Health will work toward improving recruitment, employment, development and promotional opportunities for minorities, women and other protected groups.

Scope:

All team members of Meridian Health and its partner companies, including Meridian Hospitals Corporation and its hospitals.

Policy:

Meridian Health is committed to the principles of equal employment opportunity and affirmative action and will not discriminate in the recruitment or employment practices on the basis of race, color, creed, national origin, ancestry, marital status, gender, age, religion, sexual orientation, gender identity and expression or disability and veteran status or any other protected status in accordance with all federal and state laws.

Meridian Health is committed to complying with the provisions of the Americans with Disabilities Act and will not discriminate against any qualified team member or job applicant with respect to any terms, privileges or conditions of employment because of a physical or mental disability. Meridian Health will make reasonable accommodations for eligible team members or applicants with disabilities as required by law.

Meridian Health will strive to provide equal opportunity by:

1. Maintaining an aggressive recruitment effort for minorities and women in all job categories/levels.
2. Reviewing employment requirements and practices periodically to provide that all applicants and team members are being afforded fair and equal consideration for all positions and other employment opportunities.

The policy statement on Equal Employment Opportunity will be included in the Meridian Health policy and procedure manual, will be distributed to all newly hired team members of Meridian Health, and will be posted in all areas visible to Meridian Health team members and job applicants.

Any questions regarding this policy and procedure may be referred to the Team Member and Labor Relations

Specialist, Team Member and Labor Relations Manager, Team Member and Labor Relations Senior Manager, Director of Human Resources or the Senior Vice-President of Human Resources.

Special Notes / Appendix

None

Related Documents

The following is a list of other documents related to the current document. Changes you make to the current document may affect the documents listed.

External Related Documents

N/A

Pre-PolicyStat Number: MHS-HR-01-2201

Attachments:

No Attachments

Applicability

Bayshore Medical Center, Hackensack Meridian Health Inc. , Jersey Shore University Medical Center, Legacy Meridian Health, Ocean Medical Center, Raritan Bay Medical Center - Old Bridge Division, Raritan Bay Medical Center - Perth Amboy Division, Riverview Medical Center, Southern Ocean Medical Center

HACKENSACK MERIDIAN *HEALTH*
OCEAN MEDICAL CENTER
GRADUATE MEDICAL EDUCATION
POLICIES AND PROCEDURES

Subject: **AUTOPSY**	**Policy Number:** **11.C**
Approved by GMEC: May 9, 2018	**Approved by MEC: June 7, 2018**

Reference Administrative Policy & Procedures Document #: **PolicyStat ID:** *3367545*

Effective July 1, 2018

Hackensack Meridian *Health*

Origination Date:	*06/2006*
Last Approved:	*01/2018*
Last Revised:	*03/2013*
Next Review:	*01/2021*
Owner:	*Brian Erler: Physician*
Policy Area:	*Administrative*
Applies To:	
Applicability:	*Meridian Hospitals Corporation*

Autopsy

Purpose:

To provide data for the better understanding of diseases, the advancing of medical knowledge, and the improvement of the quality of patient care.

Scope:

All clinical departments or patient care areas of Meridian Hospitals Corporation facilities, including Jersey Shore University Medical Center, Ocean Medical Center, and Riverview Medical Center.

Policy:

For certain kinds of deaths, autopsies may be required by law. For certain other kinds, autopsies are to be encouraged, but cannot be performed without the written consent of an authorized person.

A. The attending physician shall be responsible for determining whether the death is reportable to the county medical examiner (per paragraph D) for investigation and/or possible autopsy under the latter's auspices. If the death is not reportable (or if the body is released, without autopsy, by an authorized representative of the county medical examiner's office with the proper written documentation), then the attending physician shall attempt to obtain consent for an autopsy in all cases meeting any of the following criteria:

   1. Deaths in which the cause of death or a major diagnosis is not known with reasonable certainty on clinical grounds.
   2. Deaths in which autopsy may help to explain unknown and unanticipated medical complications to the attending physician.
   3. Unexpected deaths within 48 hours of a surgical or invasive procedure performed in any hospital location.
   4. Deaths associated with an adverse event including drug or transfusion related reactions.
   5. Deaths within 48 hours of discharge from the hospital or Emergency Department.
   6. DOA (Dead on Arrival) meeting the above criteria.

B. The mechanism for obtaining and documenting consent to perform an autopsy is as follows:

   1. The attending physician or his delegate shall request the consent and shall be responsible for documenting the request in the medical record. In all instances, final responsibility rests with the attending physician.

2. The consent shall be obtained from one of the following persons, in the order of priority stated, who has also assumed responsibility and custody of the body for purposes of burial or cremation:
    a. Surviving spouse
    b. Adult children
    c. Parent(s)
    d. Other next of kin (in degree of consanguinity)
    e. Absent any of the foregoing, such other person charged by law with and who has assumed responsibility and custody of the body.

    Where two or more such persons have assumed responsibility and custody of the body, the consent of any one of them is sufficient. However, the consent of both parents of a deceased newborn should be obtained, if possible. Also, an attempt should be made to resolve any disagreement among those with an equal priority.
3. Consent for autopsy shall be in writing and witnessed on the designated forms. A telephone consent is NOT acceptable. A telegram or fax is acceptable, provided its authenticity is not questionable.
4. The family may set limitations on their consent for autopsy, unless it is the medical examiner's case.
5. The chart of the deceased scheduled for autopsy is to be brought to the Admitting Office promptly with signed autopsy consent.
6. No autopsy shall be initiated until the responsible pathologist has an ample opportunity to review a written medical record. If medical record chart does not exist, the attending physician must provide a written clinical summary including, but not necessarily limited to, the specific medical indications for the autopsy request. No exception will be made to this requirement.

C. The pathologist performing the autopsy will notify the attending physician when an autopsy is to be performed.

D. Deaths reportable to the Medical Examiner: As required by the law, the following deaths shall be promptly reported to the county medical examiner by the attending who shall document such report in the record.
    1. Suspected or actual violent deaths, whether apparently homicidal, suicidal or accidental.
    2. Death not caused by readily recognizable disease.
    3. Deaths under suspicious or unusual circumstances.
    4. Deaths within 24 hours after admission to a hospital or institution.
    5. Deaths of inmates of prison.
    6. Deaths of inmates of institutions maintained, in whole or part, by the state or county where the inmate was not hospitalized therein for organic disease.
    7. Deaths from causes which might constitute a threat to public health.
    8. Deaths related to disease resulting from employment or to accidents while employed.
    9. Sudden or unexpected deaths of infants and children under 3 years of age and fetal deaths occurring without medical attendance.

E. For such reportable deaths, the matter shall abide the county medical examiner's investigation and the determination by him (and other authorized officials) whether to require an autopsy. If the medical examiner (or other authorized officials) directs an autopsy to be performed at the medical examiner's

office, no other consent is required. However, if the medical examiner instead releases the body to the next of kin without conducting an autopsy under official auspices, then the consent to an autopsy by an authorized person is required, pursuant to paragraph 2.

F. The original autopsy findings are to incorporated in the Quality Assessment and Improvement and continuing medical education programs of the medical staff.

Requirements

Definitions:

Other Authorized Officials
The state medical examiner, an assignment judge of the Superior Court, the county prosecutor, or the attorney general.

Special Notes / Appendix

Pellegrino, Ed: The Autopsy. Some Ethical Reflections on the Obligations of Pathologists, Hospitals, Families, and Society. Arch. Pathol. Lab. Med. 120:739, 1996.
Editorial: The Autopsy in Clinical Medicine. Mayo. Clin. Proc. 64:1185, 1989.
College of American Pathologists, Indications for Performing Autopsies, 1990.
Department of Laboratories Policy, Submission of Specimens for Histology, Tissue Pathology - Surgical & Autopsy Specimens, April 1999.

Related Documents

The following is a list of other documents related to the current document. Changes you make to the current document may affect the documents listed.

External Related Documents

N/A

Pre-PolicyStat Number: MHC-ADMIN-02-1034

Attachments:

No Attachments

Applicability

Bayshore Medical Center, Hackensack Meridian Health Inc. , Jersey Shore University Medical Center, Legacy Meridian Health, Ocean Medical Center, Raritan Bay Medical Center - Old Bridge Division, Raritan Bay Medical Center - Perth Amboy Division, Riverview Medical Center, Southern Ocean Medical Center

HACKENSACK MERIDIAN *HEALTH*
OCEAN MEDICAL CENTER
GRADUATE MEDICAL EDUCATION
POLICIES AND PROCEDURES

Subject: **E-MAIL, INTERNET AND WORLD WIDE WEB ACCESS AND USAGE**	**Policy Number:** **11.E**
Approved by GMEC: May 9, 2018	**Approved by MEC: June 7, 2018**

Reference Administrative I.T. Policy/ Procedure Document #: **PolicyStat ID:** *3586956*

Effective July 1, 2018

Hackensack Meridian *Health*

Origination Date:	*11/1999*
Last Approved:	*07/2016*
Last Revised:	*07/2016*
Next Review:	*07/2019*
Owner:	*Scott Fitzgerald: DIR TECHNICAL INFO SECURITY*
Policy Area:	*IT Administrative*
Applies To:	
Applicability:	*Legacy Meridian Health Group*

E-Mail, Internet and World Wide Web Access and Usage

Purpose:

This policy defines the proper use of electronic mail (e-mail), Internet services at Meridian Health. Meridian is committed to providing an environment that encourages the appropriate use of computers, the Internet, and electronic information. The utilization of computers and access to the Internet are essential tools in supporting Meridian Health work. It is the responsibility of each Meridian system user to ensure that this technology is used for proper business purposes and in a manner that does not compromise the confidentiality of proprietary, patient, or other sensitive information. This policy supplements and should be read in conjunction with Meridian's policies regarding "Sexual Harassment," "Software Licensure," and confidentiality.

Scope:

This policy applies to ALL users of Meridian's computer systems/Virtual Private Network/Internet Portals/WAN/ LANS. For the purposes of this policy, the term Users shall be defined to include employees, members of the medical staff, independent contractors, consultants, temporary workers, students, residents, and other individuals or entities who use or have access the organization's system. Meridian Health reserves the right to modify this policy from time to time.

Policy:

EMAIL USE AND PROCEDURES

- User shall only use the Meridian-approved email system when working from the Meridian secure network and for Meridian business. Access to personal or third-party email systems from the Meridian secure network is strictly prohibited.

  Exception: A variance may be granted in accordance with Meridian's Policy Variance Request procedure approved by the Director of Privacy and Data Security, and must be additionally approved in writing by the Chief Information Officer (or designee) and Meridian's Risk Department. Additional information regarding policy variances and the Variance Request Form can be obtained by contacting Privacy & Data Security.
- User shall use the same care in the tone and content of email and other electronic documents as s/he would for any other written communication. User recognizes that sending email over the Internet is instantaneous and generally irretrievable. User further recognizes that his or her email address identifies

Meridian Health and understands that any statement, even those containing a personal communications disclaimer, may be attributed to the organization. Email communications are not considered private despite any such designation either by the sender or the recipient. Meridian reserves the right to monitor its email systems – including a user mailbox – at its sole discretion in the ordinary course of business.

- User recognizes that personal email communications should not be considered to be either private or secure, and may be discoverable in compliance audits, litigation, external investigations by law enforcement personnel and internal security investigations.
- User understands that Meridian Health has the right, but not the duty, to use human or automated means to monitor, without prior notice, both individual usage and the content of all material created, stored, sent, or received on its email system and other communication systems and networks to ensure that the email is being used for legitimate business purposes and that any incidental personal use is in accordance with this policy.
- User understands that the existence of "message delete" functions do not eliminate Meridian's ability or right to access electronic communications.
- Meridian Health reserves the right to disclose facts about system usage and the content of messages to law enforcement officials and any other third parties as appropriate.
- User expressly waives any right of privacy in anything s/he creates, stores, sends, or receives on Meridian Health's computer systems or through the Internet or any other Meridian computer network, and consents to Meridian Health's access to and review of all materials created, stored, sent, or received by User.
- User shall strive to use good grammar and correct punctuation and understands that the quality of his or her writing reflects upon Meridian Health.
- Under no circumstances shall information of a confidential, sensitive or otherwise proprietary nature (including payment card information) be transmitted via email without the use of appropriate security controls put in place by the Information Technology department.
- User understands that Meridian Health owns the email system and other communications systems and networks and all messages stored on them or transmitted using them, and such communications systems may only be used to assist in the performance of User's job functions.
- At all times, User is responsible for using the email system in a professional, ethical, and lawful manner. User understands that incidental personal use of the email system is a privilege that may be revoked at any time. Occasional, limited, appropriate personal use of the email system is permitted if the user does not:
    i. interfere with the User's work performance;
    ii. interfere with any other User's work performance;
    iii. have undue impact on the operation of the organization's computer system; or
    iv. violate any other provision of this policy or any other policy, guideline, or standard of Meridian Health System.
- User understands that no right exists to obtain the contents of email communications once his or her employment/affiliation is terminated.
- User understands that log-on passwords are intended to control access to individual workstations rather than to restrict access to the content of any communications originated by User.
- Users shall not share an email password, provide email access to an unauthorized user, or access another user's email system without authorization.
- User shall be responsible for ensuring that his or her use of Meridian's email system and other communications systems and networks (including accessing email remotely) does not compromise the security Meridian Health's computer network.

- User shall be responsible for taking reasonable precautions to prevent intruders from accessing the organization's computer network without authorization and to prevent the introduction and spread of malware of any type. User shall not attempt to circumvent Meridian Health's data protection measures or uncover security loopholes or bugs.
- User shall not perform acts that waste computer resources or unfairly monopolize such resources to the exclusion of others. These acts include, but are not limited to, sending mass emails or chain email, subscribing to non business-related list servers and mailing lists, engaging in online "chat groups," or otherwise creating unnecessary network traffic. Audio, video, picture or other attached email files that require significant storage space may not be downloaded to Meridian's computer system unless such files are business related.
- Messages sent to all Meridian email users require prior approval by the Chief Information Officer or Vice President of Information Technology due to the impact mass emailing has on Meridian's computer resources.
- Email messages, which are offensive or demeaning, or disruptive to the work place, are strictly prohibited. This includes, but is not limited to, messages that are inconsistent with Meridian's policies concerning its status as an "Equal Opportunity Employer" and its policy on "Sexual Harassment." Meridian has the authority to determine what is "offensive or demeaning" or "disruptive to the work place" for the purpose of the policy.
- User shall not alter the "From" line or other attribution-of-origin information in any email message or postings. User understands that anonymous or pseudonymous electronic communications are prohibited. User further understands that the use of anonymous remailers (i.e., a mail server that receives incoming messages, removes the header information that identifies the original sender, and the sends the message to the intended recipient) is prohibited.
- Document Retention and Record Keeping – Unless directed to the contrary by his or her supervisor, User shall discard inactive email after sixty (60) days. User agrees that incoming and outgoing email communications shall be printed out or saved electronically for specified periods as necessary to meet applicable business, regulatory and legal record keeping requirements as required by his or her supervisor.
- To ensure misdirected communications are handled appropriately, User agrees to append the following footer to all email sent outside Meridian Health:

"This email and any files transmitted with @ are confidential and are intended solely for the use of the individual or entity to whom they are addressed. This communication may contain material protected by the attorney-client privilege. If you are not the intended Recipient or the individual responsible for delivering the email to the intended recipient, please be advised that you have received this email in error and that any use, dissemination, forwarding, printing, or copying of this email is strictly prohibited. If you have received this email in error, please immediately notify_____by telephone_____. You will be reimbursed for reasonable costs incurred in notifying us.

INTERNET USE AND PROCEDURES

- Meridian's network, including its connection to the Internet, is to be used for business-related purposes only and not for personal use. Any unauthorized use of the Internet is strictly prohibited. Unauthorized use includes, but is not limited to:

    1. Connecting, posting, or downloading pornographic material:
    2. sending jokes and/or cartoons;
    3. engaging in computer "hacking" and other related activities;
    4. attempting to disable or compromise the security of information contained on the computer/system;

5. otherwise using access to the Internet for personal use or for personal benefit.

- Subscriptions to news groups, list serves, and mailing lists are permitted only when the subscription is for a work-related purpose. Any other subscriptions are strictly prohibited.
- Users may NOT establish Internet or other external network connections that could allow non-users to gain access to Meridian's systems and information without the prior authorization of the CIO or Vice President of Information Technology. These connections include, but are not limited to, the establishment of hosts with public modem dial-ins, private VPN connections, home pages, and File Transfer Protocol (FTP).
- All files/email downloaded (files may only be downloaded for legitimate Meridian business purposes) must be checked for possible computer malware. Information Technology is responsible for insuring that virus and malware protection software utilized on all Meridian network attached computers is current. If uncertain whether your virus-checking software on a stand-alone computer is current, you must check with an authorized Information Technology representative PRIOR to download.
- Because postings placed on the Internet will display Meridian's address, users must make certain before posting information on the Internet the information is of a business nature, the posting is authorized, and it reflects the standards and policies of Meridian Health. Under no circumstances shall information of a confidential, sensitive or otherwise proprietary nature (including payment card information) be placed on the Internet.
- Under no circumstances may the Meridian Health logo, or "Brand " name be utilized on any web site (with the exception of the authorized MeridianHealth.com web site) unless authorized by the Meridian Vice President of Corporate Communications. All Meridian policies which apply to dissemination of information, press releases, and publicity also apply to email and Internet use.
- The use of social networking and social media on the Internet must be for approved business purposes and in accordance with Meridian's Social Media Policy (MHS-HR-01-2715A).
- User shall only use the Meridian-approved file sharing, cloud storage and file transmission procedures when working from the Meridian secure network and for Meridian business. Access to personal or third-party file sharing and transmission or cloud storage from the Meridian secure network is strictly prohibited.

  Exception: A variance may be granted in accordance with Meridian's Policy Variance Request procedure approved by the Director of Privacy and Data Security, and must be additionally approved in writing by the Chief Information Officer (or designee) and Meridian's Risk Department. Additional information regarding policy variances and the Variance Request Form can be obtained by contacting Privacy & Data Security.

SANCTIONS FOR VIOLATING POLICY

User understands that sanctions for violating Meridian Health's Email and Internet Access and Usage policy may include revocation of User's Internet and/or email privileges and disciplinary action up to and including termination of employment (or disciplinary action up to and including termination of a physician's medical staff appointment or panel participation in accordance with Meridian Health's medical staff bylaws and rules and regulations), and civil and/or criminal penalties.

Special Notes / Appendix Reference

Standard	Control	Comments
PCI-DSS v3.1	12.3.6	

Procedure:
Distribution / Routing List

All persons or areas listed below should receive a contolled copy of this document once it is approved. All members of Meridian Health workforce

Pre-PolicyStat Number: MHS-IT-0007

Attachments:

No Attachments

Applicability

Bayshore Medical Center, Hackensack Meridian Health Inc. , Jersey Shore University Medical Center, Legacy Meridian Health, Ocean Medical Center, Raritan Bay Medical Center - Old Bridge Division, Raritan Bay Medical Center - Perth Amboy Division, Riverview Medical Center, Southern Ocean Medical Center

HACKENSACK MERIDIAN *HEALTH*
OCEAN MEDICAL CENTER
GRADUATE MEDICAL EDUCATION
POLICIES AND PROCEDURES

Subject: **SMOKE-FREE WORKPLACE**	**Policy Number:** **11.G**
Approved by GMEC: May 9, 2018	**Approved by MEC: June 7, 2018**

Reference Human Resources Policies and Procedures Document #: **PolicyStat ID:** *3574197*

Effective July 1, 2018

Hackensack Meridian *Health*

Origination Date:	*05/2008*
Last Approved:	*06/2013*
Last Revised:	*06/2013*
Next Review:	*06/2016*
Owner:	*Victoria Riveracruz: SR MGR TM & LABOR RELATIONS*
Policy Area:	*Human Resources*
Applies To:	
Applicability:	*Legacy Meridian Health Group*

Smoke-Free Workplace Policy

Purpose:

It is the mission of Meridian Health to provide for the health and safety of all persons including team members, visitors/guests, patients, contractors and vendors. For safety and health reasons, Meridian will implement a smoke-free policy that prohibits the use of tobacco products (cigarettes, cigars, chewing tobacco, pipe smoking and electronic cigarettes) on hospital grounds and all off site properties owned and/or leased by Meridian Health on walkways, sidewalks, driveways and parking areas/parking garages. The use of tobacco products is prohibited in cars parked on Meridian Health property and/or in any Meridian Health vehicle. This policy becomes effective November 20, 2008.

Scope:

All team members of Meridian Health and its partner companies, including Meridian Hospitals Corporation and its hospitals. In addition, all physician/dental staff, patients, visitors/guests, vendors/contractors and volunteers are covered by this policy.

Procedure:

General Guidelines

1. All team members, physicians and dental staff will be informed of this policy through signage, policy review, general & departmental orientation, annual basic training and various communication vehicles including but not limited to plasma boards, huddles, department communication boards, the intranet, WHAM, and Drs. Notes, a publication distributed to physicians/dentists on staff with Meridian Health. The smoke-free policy will be reviewed quarterly at department staff meetings.
2. Patients, visitors/guests will be advised of the smoke-free policy prior to or upon admission to a Meridian Health facility. Team members and physicians are responsible for communicating and reinforcing this policy.
3. Volunteers, students, vendors and contractors will be informed of this policy through signage advertising or vendor contract.
4. Smoke-Free Workplace signs will be posted at all Meridian Health properties.
5. Information is available about alternatives to nicotine dependence for team members, physicians/ dentists, patients, volunteers, students, visitors and guests. Electronic cigarettes will not be allowed as an alternative during work time and/or on any company premises.

6. Based on the admitting physicians' assessment, there shall be orders for nicotine replacement therapy for patients admitted to Meridian Health.

Enforcement

1. Leaders shall ensure compliance with this policy in their respective areas.
2. In public areas, the Security team will be responsible for ensuring compliance with this policy.
3. Upon first violation, a team member may be counseled and given remediation of the smoke-free policy and resources to quit tobacco use. Team members who subsequently violate the policy may be subject to progressive discipline based on Meridian Health's Human Resources Policy Guidelines for Cooperation and Discipline.
4. All team members, leaders and physicians will ensure compliance with this policy.

   Any questions regarding this policy and procedure may be referred to the Human Resources Site Leader, the Human Resources Generalist, the Director of Human Resources, or the Senior Vice President of Human Resources.

Related Documents

The following is a list of other documents related to the current document. Changes you make to the current document may affect the documents listed.

External Related Documents

HR Policy MHS-HR-01-2602 Guidelines for Cooperation and Discipline

Pre-PolicyStat Number: MHS-HR-01-2413

Attachments:

No Attachments

Applicability

Bayshore Medical Center, Hackensack Meridian Health Inc. , Jersey Shore University Medical Center, Legacy Meridian Health, Ocean Medical Center, Raritan Bay Medical Center - Old Bridge Division, Raritan Bay Medical Center - Perth Amboy Division, Riverview Medical Center, Southern Ocean Medical Center

HACKENSACK MERIDIAN HEALTH
OCEAN MEDICAL CENTER
GRADUATE MEDICAL EDUCATION
POLICIES AND PROCEDURES

Subject: **SOCIAL MEDIA POLICY**	**Policy Number:** **11.H**
Approved by GMEC: May 9, 2018	**Approved by MEC: June 7, 2018**

Reference Human Resources Policies and Procedures Document #: **PolicyStat ID:** *3587043*

Effective Date: July 1, 2018

Hackensack Meridian *Health*

Origination Date:	*06/2010*
Last Approved:	*01/2016*
Last Revised:	*01/2016*
Next Review:	*01/2019*
Owner:	*Victoria Riveracruz: SR MGR TM & LABOR RELATIONS*
Policy Area:	*Human Resources*
Applies To:	
Applicability:	*Legacy Meridian Health Group*

Social Media Policy

Purpose:

To ensure all Meridian Health team members utilizing any form of a social media platform (i.e.: Facebook, Twitter, You Tube, Friend Feed, Blogs, Forums, Messaging Boards & Social Book Marking Sites) adhere to Meridian Health's existing policies. Team members must adhere to the following guidelines.

Scope:

All team members, physicians, volunteers or other associates of Meridian Health, its subsidiary companies, including Meridian Hospitals Corporation and its hospitals and partner companies.. This policy also applies to all applicants for employment with Meridian Health.

Policy:

Guidelines:

Team members should follow the same basic principles and policies when engaging in communication on social media or social networking platforms as in any other areas of our lives. All Meridian team members must follow other existing Meridian policies and procedures when relevant to these guidelines. The purpose of these social media guidelines is to help team members understand how Meridian policies apply to these new technologies for communication, so team members can participate with confidence by following these guidelines for social media platforms.

1. Follow All Applicable Meridian Policies.

   Communication must not contain any confidential or proprietary information of Meridian as defined below and you must maintain patient privacy and information. Communications should never contain information that identifies a patient or health condition in any way. Meridian HIPAA privacy and security policies must be at the forefront of a team member's mind when communicating on the public internet. Confidential or proprietary information includes information about trademarks, strategic plans or goals, finances, patient information or any similar information not publicly released by Meridian.

   In conformance with Meridian policy, Meridian Health team members should not engage in any form of harrassment, which may include derogatory remarks about a person's race, age, ethnicity, religion, sexual preference or health condition. Personal insults, discriminatory remarks with/or disrespect for others based on these protected traits are prohibited.

2. Write in the first person.

   Where your connection to Meridian is apparent or part of your profile in any social media or social networking site, make it clear that you are speaking for yourself and not on behalf of Meridian. In those circumstances, you may add the following disclaimer to comply with this obligation: "The views expressed on this {blog, website} are my own and do not reflect the views of my employer." Consider adding this language to the "About me" section of your blog or social networking profile.

3. Use of Meridian Health postings.

   Meridian Health team members should be conscious of differentiating between business and personal uses when utilizing social media platforms. Through social media platforms, such as Facebook, and Twitter, you may exercise your right to "share" any information or images posted by Meridian Health on its Facebook page or Twitter so long as your accompanying personal text complies with other guidelines in this policy. Always exercise good judgement and common sense.

4. Use a personal email address (not your meridianhealth.com address) as your primary means of identification.

   Meridian Health team members who communicate and engage on any social media platforms must disclose their personal identification and use a separate email other than that of a Meridian email when expressing personal views and opinions. You must not include any promotions, products, third party links in any comments, uploads or links onto Meridian sponsored social media sites.

5. Public communications about Meridian by a team member or a designated Meridian spokesperson must not harm patients or customers.

   If a Meridian Health team member is communicating about Meridian or Meridian-related matters on the internet including a Meridian-hosted site or is asked or scheduled to participate in any type of social media engagement on any platform on behalf of Meridian, the team member should disclose their connection to Meridian and role as a Meridian team member. If designated as a Meridian spokesperson, exercise good judgement and communicate accurate information. Errors or omissions by Meridian spokespersons that reflect poorly on Meridian may result in liability to you or Meridian Health.

   Disparaging or defamatory statements about Meridian patients or customers are not acceptable by anyone and team members should also avoid social media communications that might be misconstrued in a way that could damage Meridian's patients or customers.Team members also may not disclose, whether through written text, pictures, or other means confidential patient or health information.

   Team members are personally responsible for what they communicate in social media. What you publish could be available and read by the public (including Meridian, future employers and social acquaintances) for a long time. Keep this in mind before you post content.

   Meridian Health team members who participate in any form of Internet engagement on any platform a Meridian spokesperson must abide by all copyright laws when quoting text and using images. You must credit your information, text and or image from its correct source.

6. Meridian Health website or blog management.

   Meridian Health reserves the right to monitor and in its sole discretion, delete any posts, comments,

photos, videos, and audio on any social media networking site where Meridian is an administrator. Meridian reserves the right to respond, delete, revise or correct any mistakes within the form of a negative, incorrect or off topic comment on any Meridian sponsored or Internet site. Meridian reserves the right to monitor, delete, block or deny team member access to any social media site or platform at Meridian's discretion. Meridian Health will respond to any comment, post, image, text, video, email or direct message when appropriate and at its discretion.

Meridian Health reserves the right to use, copy, edit, publish or distribute any content you post on any social media platform or site where Meridian is the administrator for any purpose.

7. Each team member is expected to work in a cooperative manner with management/supervisiors, co-workers, patients and vendors.

   Meridian Health team members should not be rude, unprofessional, or uncivil to other team members, business partners, patients, and people's families when engaged in job performance or work functions.

8. Meridian-sponsored postings require approval.

   The use or creation of a profile on any external social media sites for work related purposes, such as blogs, groups forums, photo streaming sites, video, and audio must be reviewed and approved by the Meridian Corporate Communications Department. Disseminating information and/or photos from Meridian Health sponsored events, i.e., Service Award Dinners, Beach Parties, etc.on such Meridian-sponsored sites without prior approval is prohibited. Therefore, Meridian Health will not be liable for any damages, claims, losses and costs, resulting from comments, uploads, third party links, sponsored links, images, audio, video, etc.

9. Personal use of internet or email access through Meridian systems must be limited to non-working time.

   Email and internet access is provided to support Meridian Health business purposes. While team members who have access to these tools may make personal use of them during non-working time (breaks, lunches, etc. they may not make personal use of them during work time. Each team member also must comply with relevant information technology policies so as not to disrupt or impede the legitimate business purposes of the internet or email systems. See MH IT Policy re: computer/email use.

   Team Members who fail to comply with this policy shall be subject to disciplinary action, up to and including termination of employment as provided in the GUIDELINES FOR COOPERATION AND DISCIPLINE POLICY - MHS -HR-01-2602.

   Any questions regarding this policy and procedure may be referred to the Team Member and Labor Relations Specialist, Team Member and Labor Relations Manager, Team Member and Labor Relations Sr. Manager, Director of Human Resources or the Senior Vice President of Human Resources.

Related Documents

The following is a list of other documents related to the current document. Changes you make to the current document may affect the documents listed.

External Related Documents

Meridian Health Confidentiality Policy #MHC-Admin--02-1084

Media Relations - MHS-Admin-01-1059
Information Systems - Integrity Policy - IT-SEC-004
Email, Internet and World Wide Web Access and Usage - MHS-IT-0007

Pre-PolicyStat Number: MHS-HR-01-2715A

Attachments:

No Attachments

Applicability

Bayshore Medical Center, Hackensack Meridian Health Inc. , Jersey Shore University Medical Center, Legacy Meridian Health, Ocean Medical Center, Raritan Bay Medical Center - Old Bridge Division, Raritan Bay Medical Center - Perth Amboy Division, Riverview Medical Center, Southern Ocean Medical Center

HACKENSACK MERIDIAN *HEALTH*
GRADUATE MEDICAL EDUCATION
POLICIES AND PROCEDURES

Subject: **MOBILE AND ELECTRONIC DEVICES**	**Policy Number:** 11.I
Approved by GMEC: May 9, 2018	**Approved by MEC: June 7, 2018**

Reference: MH Privacy and Data Security Policy/Procedure #: **PolicyStat ID:** *4657047*

Hackensack Meridian *Health*

Origination Date:	*02/2012*
Last Approved:	*03/2018*
Last Revised:	*03/2018*
Next Review:	*02/2021*
Owner:	*Scott Fitzgerald: DIR TECHNICAL INFO SECURITY*
Policy Area:	*IT Security*
Applies To:	*Hackensack Meridian Health Network*
Applicability:	*Legacy Meridian Health Group*

Electronic Information Use at Hackensack Meridian Health

Purpose:

This policy is a point of reference for Hackensack Meridian System Users (defined below) regarding the appropriate use of and access to Hackensack Meridian *Health* Information (See definition below).

Scope:

All Hackensack Meridian *Health* team members, members of the medical and dental staff, volunteers, students, business associates, partner companies and vendors, collectively referred to as "Hackensack Meridian System Users".

Policy:

The Hackensack Meridian *Health* information system network is a "protected" environment, and Meridian System Users must follow this policy and the policies referenced below in order to keep Hackensack Meridian Information within the protected environment. Hackensack Meridian System Users shall maintain the security of Hackensack Meridian Information so that Hackensack Meridian Information is accessed and maintained securely.

Hackensack Meridian System Users must use the HMH Portal when accessing Hackensack Meridian Information from a non-HMH location (i.e. working remotely).

Access or Use of Hackensack Meridian Information from a non-HMH location:

All Hackensack Meridian System Users are expected to understand and follow the points stated below:

1. All Hackensack Meridian System Users that work offsite or away from their usual workstation (at a non-HMH location) must be authorized to have remote access by their manager (or a member of the hospital or corporate administration) and only access Hackensack Meridian Information via the HMH Portal.
2. Hackensack Meridian system users may not connect, use, store, copy, transfer or send Hackensack Meridian Confidential and Protected Information on any removable media or cloud service without specific approval from Hackensack Meridian's Privacy & Data Security Officer.
3. Documents containing Hackensack Meridian Confidential Information stored on removable media must only be on a Hackensack Meridian issued encrypted flash drive, and may only be stored there after obtaining specific approval from Hackensack Meridian's Privacy & Data Security Officer.

4. A Hackensack Meridian System user must have a password protected mobile device with encryption enabled (i.e. cell phone, smart phones, PDA or tablet) in order to use or store Hackensack Meridian Information such as email or confidential information on a mobile device.
5. Hackensack Meridian Confidential and Protected Information may only be printed at Hackensack Meridian locations. Hackensack Meridian Confidential and Protected Information must not be printed from a non-HMH location. Hackensack Meridian System Users are responsible for protecting and safeguarding information in accordance with Hackensack Meridian policies.
6. Printing of business information that is Confidential Information is permitted from a non-HMH location if you are authorized to have and use the information in order to perform your job duties and such information does not include PHI, ePHI, PII or PCI data.

Any exception to this policy requires prior written approval from Hackensack Meridian's Privacy & Data Security Officer. Exceptions will be granted only in extraordinary circumstances.

Electronic Information Use Policies:

All of the policies below relate to electronic information use at Hackensack Meridian and must be reviewed and followed by the Hackensack Meridian System User.

Each policy is located on the Hackensack Meridian intranet in the policy and procedure section with the policy number noted below. Please note, the below policy summaries are for your reference. If the policy summary is different than the original fully approved policy, the fully approved policy is what Hackensack Meridian System Users must follow.

To access any of the policies electronically, click on the policy named below and you will be automatically routed to the policy on the Hackensack Meridian intranet. For ease of review, the policies according to category are listed as follows:

1. **Confidentiality of Information Policies**

   Use of Social Security Numbers MHS-ADMIN-01-1066
   Social Security numbers will be used in accordance with regulations set forth by the N.J. Identity Theft Protection Act. Social Security numbers will not be used to identify individuals in Hackensack Meridian information systems except where required by Federal or State law or legally enforceable rule or regulation.

   Usage of Mobile Devices/Removable Media **MHS-PRI-0049**
   The purpose of this policy is to outline the appropriate usage and type of mobile devices and removable media that may be used with Hackensack Meridian Information. Hackensack Meridian Information includes any and all Hackensack Meridian work product/documents, confidential information, HMH clinical data or records, personally identifiable information and electronic protected health information (See definitions below). Hackensack Meridian System Users shall not save, copy, transfer or otherwise retain any Hackensack Meridian Information onto any mobile device/removable media (See definitions below).

   Non-Disclosure of Information MHS-IT-0025
   The purpose of this policy is to ensure that team members treat all information contained in or produced by all computer systems with strict confidentiality and will not disclose system information to anyone except as required by their job.

Disclosures of De-identified Health Information and Creation of a Limited Data Sets MHS-PRI-0018
Hackensack Meridian *Health* is required by the Federal Health Insurance Portability and Accountability Act of 1996 and its related regulations ("HIPAA") to maintain the confidentiality and privacy of a patient's identifiable health information ("Protected Health Information" or "PHI"). This policy explains how Hackensack Meridian determines whether a patient's PHI is (i) identifiable and required to be protected, or (ii) is sufficiently de-identified so that it is not subject to confidentiality and privacy rules. This policy also explains under what circumstances de-identified health information ("De-identified Health Information") may be re-identified by Hackensack Meridian. This policy also explains (i) the method by which a limited data set of patient health information can be created, and (ii) the circumstances under which limited data sets can be used and disclosed for research, public health and health care operations purposes.

Emergency Access to Systems Housing EPHI MHS-PRI-0035
This policy establishes the methodology for granting access to systems containing "EPHI" in emergency or other unusual situations, including temporary and disaster credentialing of Independent Licensed Practitioners. The rule of "least privileged" access shall be followed while providing the level of access required to perform job functions when emergency circumstance or other unusual circumstances exist.

Permitted Uses and Disclosures of Patient Information MHS-PRI-0019
This policy establishes the general rules which Meridian will follow when using and disclosing the health information of its patients. All Hackensack Meridian team members are expected to maintain the confidentiality and privacy of patient information in accordance with the Federal HIPAA Law.

2. **Protection of Information Policies**

Breach Notification (Protected Health Information) MHS-PRI-0040
Hackensack Meridian *Health*, a HIPAA Covered Entity, will notify affected individuals and applicable government agencies, as soon as possible, but in no event more than 60 days after the discovery of a Breach of Unsecured Protected Health Information in accordance with the requirements of the HITECH Act and the NJ Identity Theft Prevention Law.

Privacy and Security Incidents – Response and Reporting Policy
This policy describes the process team members should follow to respond to a computer generated alert related to a privacy or security incident and to report a privacy and security incident. Privacy and Security incidents may include loss, access or unauthorized disclosure of confidential information, protected health information, personally identifiable information, electronic PHI or ePHI, (collectively "Hackensack Meridian Information"), which may be contained on computer equipment, portable devices or equipment, or contained in documents and oral communications.

Password Management for Systems Containing Electronic Protected Health Information MHS-PRI-0030
This policy establishes the requirements for the creation, revision, and management of passwords that are used to gain access to Hackensack Meridian Information or a Biomedical System containing Protected Health Information.

PDA - Personal Digital Assistant Policy MHS-IT-0040
This policy establishes the requirements for authorized access to synchronize a PDA with Hackensack Meridian's Email service. The purpose of this policy is to maintain network security. PDA's are not permitted to synchronize with Hackensack Meridian *Health's* networked workstations by either "docking"

or directly connecting them to the workstation. ALL MOBILE DEVICES (CELL PHONE, PDA, TABLET, ETC.) THAT CAN ACCESS THE HACKENSACK MERIDIAN EMAIL SYSTEM MUST BE PASSWORD PROTECTED AT ALL TIMES. THE HACKENSACK MERIDIAN SYSTEM USER IS RESPONSIBLE FOR ENSURING THAT SAID MOBILE DEVICES ARE PASSWORD PROTECTED.

Transmission Security Policy MHS-PRI-0037

The purpose of this policy is to ensure the security and compliance of information entrusted to or owned by Hackensack Meridian *Health* when it is sent in motion, whether internally or beyond the boundaries of Hackensack Meridian *Health's* IT private network. This policy documents the authorized methods which may be used and the security measures enacted to guard against unauthorized access or modification of protected health information or personally identifiable information transmitted on Hackensack Meridian *Health's* internal network and sub-networks or to points outside of the Hackensack Meridian *Health* network.

Vendor Non-Disclosure of Confidential Information MHS-IT-0018

Patients' financial, clinical and administrative information contained within Hackensack Meridian *Health's* various computer systems is considered highly confidential. As such, great care should be taken to maintain the confidentiality and security of data.

Contracts for companies providing information technology products and services to Hackensack Meridian *Health* will include specific privacy and security requirements.

Facsimile Transmissions of Health Information MHS-PRI-0005

This policy concerns the authorized manner and process for transmitting protected health information via facsimile (fax) transmission.

3. **Clinical Trials and Research Policies**

The Hackensack Meridian *Health* Institutional Review Board ("IRB") Policy & Procedure **IRB-ADM-02-0001**

The Institutional Review Board policy contains a link to the policy manual for all Hackensack Meridian System Users who are involved in research or clinical trials. The policy manual in conjunction with the above policies should be used as a reference to those Hackensack Meridian System Users conducting human subject research.

4. **System Access and Usage Policies**

Remote Access Policy IT-SEC-0060

The purpose of this policy is to define standards for connecting to Hackensack Meridian *Health's* network from any remote location. These standards are designed to minimize the potential exposure to Hackensack Meridian *Health* from damages which may result from unauthorized use of Hackensack Meridian *Health* resources.

Automatic Logoff Policy MHS-PRI-0036

The purpose of this policy is to ensure that access to all servers and workstations that access, send, receive, or store EPHI is appropriate and that there are controls in place to automatically log users off to prevent unauthorized access.

Acceptable Use Policy
This policy defines the proper use of electronic mail (e-mail), Internet and technology at Hackensack Meridian *Health*. Hackensack Meridian *Health* is committed to providing an environment that encourages the appropriate use of computers, the Internet and electronic information.

Redirection of Email Policy MHS-IT-0028
Non-HMH email accounts, including those that are the personal email accounts of members of the Hackensack Meridian Workforce, are not to be used to conduct Hackensack Meridian *Health* business. Those individuals who need to access/send business related emails from remote locations shall do so through the Hackensack Meridian Application Portal or Hackensack Meridian Web mail.

Media Controls for Disposal and Re-Use MHS-PRI-0034
The purpose of this policy is to ensure that Hackensack Meridian *Health* controls the re-use and disposal of all devices and other media containing Electronic Protected Health Information or EPHI.

Computer Virus/Worm Protection MHS-IT-0004
This policy provides details regarding the prevention and passing of computer viruses between computers, PDA's/servers/etc. THIS INCLUDES ANY AND ALL COMPUTERS, SERVERS, ETC. ATTACHED TO, OR AS PART OF, BIO-MEDICAL/SECURITY/DISPENSING EQUIPMENT.

Non-HMH Devices Connection to Network MHS-IT-0036
This policy does not allow non-HMH devices to connect to the Hackensack Meridian network. A Hackensack Meridian device may NOT be disconnected from the network to allow any non-HMH device connection to the network.

Performance Evaluation

Consequences: Members of the workforce who fail to comply with this policy shall be subject to sanctions, up to and including termination of employment.

Definitions:

See Information Governance Definitions MHS-IT-0072.

Acknowledgment:

Hackensack Meridian System Users will acknowledge their understanding of the Hackensack Meridian Privacy & Data Security policies upon the first request for system access and on an ongoing basis annually in order to maintain their access to Hackensack Meridian systems and the Hackensack Meridian network. Any non-HMH employed users must acknowledge their understanding prior to system access being provided.

Questions:

Questions regarding this policy are to be directed to the Hackensack Meridian Privacy & Data Security Officer at (732) 751-3448.

References

Standard	Control	Comments
PCI-DSS v3.1	7.3 12.3.5	

Pre-PolicyStat Number: MHS-PRI-0044

Attachments:

No Attachments

Approval Signatures

Step Description	Approver	Date
	Scott Fitzgerald: DIR TECHNICAL INFO SECURITY	03/2018

Applicability

Bayshore Medical Center, Hackensack Meridian Health Inc. , Jersey Shore University Medical Center, Legacy Meridian Health, Ocean Medical Center, Raritan Bay Medical Center - Old Bridge Division, Raritan Bay Medical Center - Perth Amboy Division, Riverview Medical Center, Southern Ocean Medical Center