Uses and Disclosures of Protected Health Information

Purpose:

To provide guidance on the appropriate uses and disclosures of Protected Health Information (PHI) for all employees.

Policy: EOMC will use and disclose Protected Health Information contained in a designated record set as required by and in compliance with the privacy regulations and state law.

Procedure:

1. De-identified health information and limited data set information

    a. Health information that has been de-identified is no longer considered protected health information and cannot be re-identified.

    b. De-identification consists of removal of the following identifiers of the individual or of relatives, employers, or household members of the individual:

        i. Names

        ii. Geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code

        iii. All elements of dates, except year, for dates directly related to an individual, including birth date, admission date, discharge date, date of death

        iv. Telephone numbers

        v. Fax numbers

        vi. Electronic mail addresses

        vii. Social security numbers

        viii. Medical record numbers

        ix. Health plan beneficiary numbers

        x. Account numbers

        xi. Certificate/license numbers

        xii. Vehicle identifiers and serial numbers, including license plate numbers

        xiii. Device identifiers and serial numbers

        xiv. Web universal resource locators (urls)

        xv. Internet protocol (IP) address numbers

        xvi. Biometric identifiers, including finger and voice prints

        xvii. Full-face photographic images and any comparable images

xviii. Any other unique identifying number, characteristic, or code.

c. Information that is contained in a limited data set may be used or disclosed in conjunction with a limited data set agreement when the above direct identifiers of the individual or of relatives, employers, or household members of the individual have been eliminated.

2. Minimum necessary

a. EOMC will only disclose the minimum amount of PHI necessary to accomplish the intended purpose of the use or disclosure.

b. EOMC will independently determine the necessary minimum disclosure and will verify that only the minimum necessary information is used or disclosed.

c. This minimum necessary requirement does not apply to uses and disclosures of PHI to the patientfor treatment, pursuant to an authorization, a disclosure required by law, a disclosure to a health oversight agency, a disclosure necessary to comply with the privacy rule, or a disclosure to the Secretary of Health and Human Services.

d. EOMC will identify persons in the workforce and other persons (medical staff, business associates) who require access to PHI to carry out their specific duties and will take reasonable steps to limit access to PHI for those individuals or categories of individuals in carrying out their duties.

3. Verification

a. When a disclosure of PHI is conditioned upon particular documentation, statements, or representations, prior to the disclosure of the PHI, the identity of the person making the request and the authority of the person to make the request shall be verified.

b. Verification may consist of written representations, verbal representations and personal knowledge.

c. EOMCmay rely upon the representations and documentation provided to it, if the reliance is reasonable under the circumstances (for example, a law enforcement officer’s badge or a letter written on agency letterhead).

4. Incidental disclosures

a. An incidental disclosure is a disclosure that is a by-product of an authorized use or disclosure of PHI.

b. It is a disclosure that is limited in nature and cannot be reasonably prevented. i. Example: posting the name of a patient on a white board or maintaining a sign in sheet.

c. Prior to making an incidental disclosure, the employee or business associate will verify that the disclosure cannot reasonably be prevented or minimized.

5. Authorization

a. When a use or disclosure is not otherwise permitted under these policies, EOMCwill secure a valid authorization prior to making any use or disclosure of PHI.

b. IfEOMC sells PHI, or otherwise uses or disclosures PHI for marketing purposes, an authorization will be secured prior to such sale or use/disclosure for marketing purposes. [see Authorization to Use and Disclose Protected Health Information.]

6. Uses and disclosures for treatment, payment, and healthcare operations

a. No authorization is necessary for uses and disclosures of PHI for the patient’s treatment, for payment of the patient’s treatment or for EOMC’s healthcare operations.

i. Healthcare operations include quality assessment and improvement activities such as:

1. Evaluations and development of clinical guidelines (provided that the obtaining of generalized knowledge is not the primary purpose for these studies)

2. Population-based activities relating to improving health care or reducing health care costs, protocol development, case management and care coordination

3. Contacting providers and patients about treatment alternatives

4. Activities of patient safety organizations

5. Reviewing the competence and qualifications of health care professionals

6. Evaluating health plan, practitioner, and provider performance

7. Conducting training programs in which students and trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers

8. Training of non-health care professionals

9. Accreditation, certification, licensing, and credentialing

10. Underwriting, premium rating, or activities relating to the creation, renewal or replacement of a health insurance or benefits contract

11. Medical reviews

12. Legal services

13. Auditing functions (including fraud and abuse, compliance programs)

14. Business planning, business development, cost planning and management-related analysis of the entity's operations

15. Formulary development and administration

16. Development or improvement of methods of payment or coverage policies

17. Business management

18. General administrative activities

19. Customer service

20. Resolution of internal grievances

21. Activities related to the sale, transfer or merger of the covered entity

7. Uses and disclosures for the facility directory

a. No authorization is necessary andEOMCmay include a patient in the facility directory when the patient has not objected to his/her name, location in the hospital, general condition (in general terms – good, fair, serious and critical), and religious affiliation being included in the directory after having been provided an opportunity to object.

b. Once included in the facility directory, the patient's name, location in the hospital, and condition in general terms may be disclosed to individuals who inquire about the patient by name, and members of the clergy may obtain the patient's name, location in the hospital, condition in general terms, and religious affiliation.

8. Uses and disclosures to individuals involved in the patient's care (including decedents) or for disaster relief

a. No authorization is necessary, and PHI may be used or disclosed, to:

i. Any person identified by the patient (or the personal representative) as being involved in his/her care, including a “support person”

ii. Notify a family member, personal representative, or other person responsible for the care of the patient of his/her location, general condition, or death

iii. A disaster relief organization. To make such disclosure:

1. The person must be present during the health care communication and the patient must not object to his/her presence.

2. The patient must agree to the disclosure or it is reasonable to infer (based upon the provider’s professional judgment) from the circumstances that the patient would not object to the disclosure.

3. If the patient is not present or is not able to object, a disclosure may be made when, in the professional judgment of the provider, the disclosure is in the patient’s best interests.

4. Disclosures must be limited to information directly related to the individual’s involvement in the patient’s care.

iv.PHI about a decedent may also be released to family members or individuals involved in the patient’s careor payment for care prior to death, unless doing so is inconsistent with any known prior expressed preference of the decedent.

1. The disclosure is limited to the family member’s or other individual’s actual involvement in the patient’s care or payment for care.

i. Example:EOMCcould describe the circumstances that led to the decedent’s death with the decedent’s sister who asks about her sibling’s death.

ii. It is also appropriate to disclose billing information to a family member that is assisting with the decedent’s estate. The disclosure will not include information about past, unrelated medical problems.

v. Prior to making a disclosure about a decedent, EOMC will obtain reasonable assurances that the family member or individual requesting the PHI was involved in the patient’s care or payment for care prior to the decedent’s death.

1. Example: the family member or individual may be asked to provide information concerning how he/she is related to the decedent or details about the decedent’s condition prior to his/her death.

9. Uses and disclosures required by law

a. EOMC may use and disclose PHI without authorization when the disclosure is required by federal or state statute or regulation and the disclosure complies with and is limited to the requirements of the law.

b. The particular privacy requirements pertinent to those subjects (and as described in this policy) must be met if the disclosure:

i. Involves adult abuse, neglect or domestic violence

ii. Involves judicial or administrative proceedings

iii.Is for law enforcement purposes

10. Uses and disclosures for public health activities

a. A public health authority is an authority mandated by law or regulation to collect or receive information to prevent or control disease, injury, disability, or to conduct public health surveillance, investigations, or interventions.
b. EOMCmay use and disclose PHI without authorization to a public health authority for public health activities.
c. Public health activities include but are not limited to:
    i. Reporting specific diseases and conditions
    ii. Reporting births and deaths for vital statistics
    iii. Reporting child/adult abuse and neglect
    iv. Reporting FDA-regulated products or activities
    v. Reporting persons exposed to or at risk for contracting or spreading communicable diseases.
    vi. When the patient is provided with a written communication prior to treatment, PHI may be disclosed without authorization to an employer when the treatment is provided to the patient at the employer's request for a work-related illness or injury, for workplace related health surveillance, or for OSHA compliance

11. Uses and disclosures of immunizations

a. EOMC may disclose immunization information to a school upon the written or verbal consent of a parent, guardian, or person acting in place of the parent (pursuant to the parent's direction).
b. This consent must be documented in the child's health record.
    i. Example: if the parent submits a letter or email request to EOMCfor the disclosure of the child's immunization records to the child's school, a copy of the letter or email will be maintained in the child's health record.
    ii. If the parent calls the office and requests over the telephone that his/her child's immunization records be disclosed to the minor's school, EOMCwill make a notation in the minor's health record of the telephone call.
        1. The notation must include the time the telephone call was received
        2. The workforce member who took the telephone call
        3. The workforce member who logged the telephone call into the child's health records
        4. A general description of the request

12. Uses and disclosures about victims of abuse, neglect, or domestic violence

a. EOMCwill report child and adult abuse as required by law. No authorization is necessary to use and disclose PHI for reporting abuse or neglect.
b. Child abuse reports
    a. When EOMChas reason to suspect that a child has been injured as a result of physical, mental, or emotional abuse, neglect, or sexual abuse, EOMCwill report the suspected abuse or neglect to law enforcement or other proper authorities.
    b. The report must include:
        1. Name of child
        2. Address
        3. Location
        4. Names of persons responsible for child and their addresses
        5. Gender
        6. Race
        7. Age
        8. Reasons why the reporter suspects the child may be in need of care
        9. Nature and extent of harm to child, including evidence of previous harm
        10. Any other information the reporter believes is helpful to establish the cause of harm

c. Adult abuse reports
    i. When EOMChas reason to suspect that an individual over the age of 18 who is cared for in a facility or the home of a family member, friend, or caretaker, EOMC will report the suspected abuse or neglect to law enforcement or other proper authorities.
    ii. Receives community services funded by the state
    iii. An individual who is over the age of 18 who is unable to otherwise protect his/her own interests, has been abused, neglected, exploited, is in a condition that is the result of abuse, neglect, or exploitation
    iv. Is in need of protective services, EOMCwill report the suspected abuse or neglect to law enforcement or other proper authorities.
    v. The report must include:
        1. The name and address of the reporter
        2. Name and address of the caretaker of the individual
        3. Information regarding the nature and extent of abuse, neglect or exploitation
        4. Name of next of kin
        5. Any other information the reporter believes might be helpful in an investigation of the case and the protection of the individual.

d. In addition to mandated child and adult abuse or neglect reports, EOMC may disclose PHI to report child or adult abuse or neglect without authorization:
    i. When the patient/personal representative agrees to the disclosure and the agreement is documented in the health record.
    ii. When the disclosure is authorized by statute and EOMCbelieves the disclosure is necessary to prevent serious harm to the patient or another potential victim.
    iii. When the disclosure is authorized by statute and the patient is unable to agree because of incapacity.
    iv. When the agency or law enforcement official receiving the report agrees not to use the information against the patient and the reporter believes that immediate law enforcement activity is necessary and cannot wait for patient/personal representative agreement.
    v. And, unless the patient would be placed at risk of harm or the personal representative is believed to be the perpetrator of the abuse or neglect, EOMCmust inform the patient/personal representative of the disclosure.

13. Uses and disclosures for health oversight activities

a. A health oversight agency is an agency of the United States, a state, a political subdivision of a state, aNative AmericanTribe, or any person, contractor, or entity acting on its behalf.
b. EOMC may use and disclose PHI without authorization to a health oversight agency for its oversight activities including:
    i. Audits
    ii. Civil
    iii. Criminal
    iv. Administrative investigations
    v. Inspections
    vi. Licensure
    vii. Disciplinary actions
    viii. Determinations of regulatory compliance

c. Authorization is necessary when:

    i. The patient is the subject of an investigation and the investigation does not arise out of or is not directly related to the delivery of health care services to the patient

ii. A health care related claim for public benefits is made and the patient's health is integral to the claim

iii. The patient qualifies for or receives public benefits.

14. Uses and disclosures for judicial and administrative proceedings

a. EOMCmay use and disclose PHI (except substance abuse treatment records and psychotherapy notes) when the information is requested for judicial or administrative proceedings.
b. To disclose PHI without authorization the patient's condition is an issue in the proceeding and:
    i. There is a court order (approved and signed by a judge) authorizing the disclosure of PHI
    ii. A judge has signed a subpoena requiring the production of PHI
    iii. A district attorney or attorney general has issued a subpoena for a properly formed inquisition or investigation
    iv. A subpoena or other discovery request has been issued, and there are satisfactory assurances accompanying the subpoena or discovery request in the form of a written statement and supporting documentation that show:
        1. The requesting party has notified the patient of the request for his/her PHI
        2. The requesting party has provided sufficient information so the patient could object to the request
        3. The time to object has passed without the patient making an objection or the court has ruled on an objection in favor of the requestor
    v. The parties in the legal proceeding have agreed to a protective order and have presented a protective order to the court and the subpoena or other discovery request contains a copy of the proposed order and the proposed order prohibits the parties from disclosing the PHI for any purpose other than the judicial proceeding and requires the parties destroy or return the PHI at the end of the case
c. Substance abuse treatment recordsof providers may only be disclosed without an authorization when there is a court order and a subpoena.
d. In civil cases:
    i. The order must limit disclosure to parts of the patient record necessary to fulfill the objective of the order and limit disclosure to persons whose need for the information is the basis for the order.
    ii. The order must contain findings that the disclosure is necessary.
    iii. Other ways of obtaining the information are not effective or would not be available.
    iv. The public interest or need for the disclosure outweighs the potential injury to the patient or the physician-patient relationship.
e. In criminal cases:
    i. The order must limit disclosure to parts of the patient record necessary to fulfill the objective of the order
    ii. The order must limit disclosure to those law enforcement and prosecution officials who are responsible for conducting the investigation or prosecution
    iii. The order must limit use of the records to investigation and prosecution of an extremely serious crime or suspected crime
    iv. The order must contain findings that the crime is serious
    v. There is a reasonable likelihood that the records will disclose information of substantial value to the investigation or prosecution
    vi. Other ways of obtaining the information are not effective or would not be available
    vii. The potential injury to the patient or the physician-patient relationship is outweighed by the public interest and need for disclosure

viii. If the applicant for the order is a law enforcement official that the entity holding the records has been afforded the opportunity to be represented by counsel

15. Uses and disclosures for law enforcement purposes

a. EOMC may use and disclose PHI without authorization to a law enforcement official, state attorney general, district attorney or police officer:
    i. To report suspected child or adult abuse
    ii. To report bullet wounds, gunshot wounds, powder burns, injuries caused by discharge of a firearm, knife wounds, or wounds from other sharp objects which are likely to result in death
    iii. To report a death that is the result of criminal activity
    iv. To report criminal conduct on EOMC's property
    v. To alert law enforcement officials about a crime which was not committed on EOMC's property, when the information comes from the provision of emergency treatment
        1. The information reported may include:
            a. The location of the crime
            b. Victims of the crime
            c. The identity of the alleged perpetrator
            d. A description of the alleged perpetrator
            e. The location of the alleged perpetrator
    vi. When a law enforcement officer requests information to identify or locate a suspect, fugitive, missing person, or material witness
        1. The information disclosed must be limited to:
            a. Name
            b. Address
            c. Date of birth
            d. Blood type
            e. Type of injury
            f. Distinguishing characteristics
            g. Date of treatment
            h. Time of treatment
            i. Date of death
            j. Time of death
    vii. When a patient is the victim of a crime and a law enforcement official requests information
        1. The patient agrees to the disclosure of information
        2. If the patient is not able to agree:
            a. The law enforcement officer denotes that the information is necessary to determine if a crime has been committed by someone other than the patient
            b. That delay in obtaining the information would adversely impact law enforcement activity
            c. EOMCdetermines in its professional judgment that disclosure is in the best interests of the patient
b. The patient's health information should contain documentation of law enforcement disclosures.

16. Uses and disclosures about decedents

a. EOMC may, without authorization, use and disclose PHI to a coroner or medical examiner to determine the identity of the decedent and/or determine the cause of death.
b. EOMCmay, without authorization, disclose PHI to a funeral director to carry out his/her duties.
c. EOMC may, without authorization, disclose information to family members and individuals involved in the decedent's care provided the disclosure is limited to the family member or other individuals involved in the

care

d. A decedent's protected health information is no longer protected by the privacy regulations after fifty (50) years from the date of death

17. Uses and disclosures for organ donations

    a. EOMCmay, without authorization, use and disclose PHI to an organ procurement organization or entity engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating donation and transplantation.

18. Uses and disclosures to avert serious threats to health and safety

    a. EOMCmay, without authorization, use and disclose PHI whenEOMC in good faith believes the use or disclosure is necessary to lessen or prevent a serious and imminent threat to the health or safety of a person and
        i. The use or disclosure is made to a person or entity that is able to prevent or lessen the threat, including the target of the threat
        ii. The use or disclosure is necessary for law enforcement to identify or apprehend an individual based upon that individual making a statement which admits participation in a violent crime which may have caused serious physical harm to the victim
        iii. When it appears from all the circumstances that the individual has escaped from a correctional institution or law enforcement custody
        iv. Unless EOMClearns about this information during a course of treatment to affect the propensity to commit the criminal conduct that is the basis for the statement
        v. Or person making the statement is seeking to initiate treatment or be referred for treatment for the type of conduct that is the basis for the statement
    b. EOMC may only disclose
        i. Name and address
        ii. Date and place of birth
        iii. Social security number
        iv. Blood type
        v. Type of injury
        vi. Date and time of treatment
        vii. Date and time of death
        viii. Description of distinguishing characteristics.

19. Uses and disclosures for special government functions

    a. EOMC may use and disclose without authorization:
        i. PHI of armed forces personnel to military command authorities for activities necessary for proper execution of the military mission
            1. If a patient is a component of the department of defense, EOMCmay use and disclose the PHI of a veteran or of a member of the armed forces upon separation or discharge to the department of veteran's affairs for a determination of eligibility or entitlement for veteran's benefits
        ii. PHI of a member of a foreign military force to a foreign military authority for proper execution of the military mission
        iii. To authorized federal officials to conduct lawful intelligence and counter-intelligence activities authorized by the national security act
        iv. To authorized federal authorities for the security and protection of the president, other individuals who are provided federal protective services, or foreign heads of state provided protective services
        v. To determine medical suitability for a state department security clearance

vi. To determine medical suitability for foreign service
vii. To determine medical suitability for a family member to accompany a member of the foreign service abroad.

20. Uses and disclosures to correctional institutions or about persons in law enforcement custody

a. EOMC may use and disclose without authorization the protected health information of a person who is in custody or who is presently incarcerated to a correctional facility or law enforcement official when
i. The disclosure is necessary to treat the person
ii. The information is necessary to protect the health and safety of other inmates, persons, or employees at the correctional facility or who transport the person.

21. Uses and disclosures for workers compensation

a. EOMCmay use or disclose without authorization PHI for treatment related to a worker's compensation claim when the disclosure is made to the
i. Patient
ii. Employer
iii. State division of worker's compensation
iv. Parties to the worker's compensation proceeding
v. Third party worker's compensation payer
vi. Individuals providing treatment.

Violations:

1. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Mobile Devices Policy

Purpose:

To allow for the authorized use of smartphones and other portable computing and communications devices at EOMC by authorized members of the EOMC Workforce.

General Information:

Mobile Devices can be used to provide better health care and more efficient administration in health care organizations. At the same time, the use of such devices creates new risks to patient privacy, Protected Health Information (PHI) and employee and organizational confidentiality, and intellectual property. This Policy is intended to permit the use of such devices while managing the risks they present.

Definitions:

1. Electronic Protected Health Information (ePHI): Individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.
2. User:Any employee or other person authorized by EOMC toread, enter or update information created or transmitted via theelectronic system.
3. Mobile Devices: Includes, but is not limited to smartphones, portable hard drives and USB (thumb) drives,digital music players, hand-held computers, laptop computers, tablet computers, and personal digital assistants (PDAs).

Procedures:

1. This Policy applies to all electronic computing and communications devices which may be readily carried by an individual and is capable of storing, receiving, processing, or transmitting digital information, whether directly through download or upload, text entry, photograph or video, from any data source, whether through wireless, network or direct connection to a computer, other Portable Device, or any equipment capable of recording, storing or transmitting digital information (such as copiers or medical devices).
2. Office and medical equipment capable of recording, storing or transmitting digital information, such as imaging equipment or copiers, are not Mobile Devices subject to this Policy.
3. This Policy applies to personally owned Mobile Devicesas well as Mobile Devices owned or leased and provided by EOMC.
4. Prohibited Mobile Devices.
    a. Mobile Devices which may produce electromagnetic interference with medical devices or equipment, or which cannot be or have not been configured to comply with this Policy, are prohibited.
5. In order to maintain the confidentiality and integrity of the Mobile Devices, EOMC will (choose what best fits your organization):
    a. Keep an inventory of all mobile devices used by healthcare professionals to access and transmit ePHI.
    b. Store mobile devices, when not in use, in locked offices or lockers.
    c. Use remote shutdown tools to prevent data breaches by remotely locking mobile devices.
    d. Install and regularly update anti-malicious software (also called malware) on mobile devices.
    e. Install firewalls where appropriate.
    f. Install IT backup capabilities, such as off-site data centers and/or private clouds, to provide redundancy and access to electronic health information.
    g. Adopt biometric authentication tools to verify the user is authorized to access the ePHI.
    h. Ensure mobile devices use is secure, encrypted Hypertext Transfer Protocol Secure (“HTTP”) similar to those used in banking and financial transactions to provide encrypted communication and secure identification of a network web server.
    i. Use of portable devices shall employ approved EOMC VPN technology when establishing communication links.
    j. Mobile devices accessing wireless networks must meet the following criteria:
        i. Mobile devices must use encryption for secure information transfers.
        ii. Portable devices using only WEP encryption technology will not be approved for the transfer of ePHI or other sensitive information.
        iii. Portable devices using publicly accessible wireless infrastructures and accessing ePHI or other sensitive information shall employ two factor authentications as defined in accordance with EOMCpractices.

k. System Administrators shall ensure that ePHI or other sensitive information subject to final disposition is disposed of by using a method that ensures the ePHI or other sensitive information cannot be recovered or reconstructed.
    i. The Security Officer shall maintain documentation of such data destruction that lists the device, the date of destruction, the workforce personnel authorizing the destruction, general description of the ePHI or other sensitive information (if available), and the identity of the workforce personnel performing the destruction.

6. Authorization to Use Mobile Devices.
    a. No Mobile Device may be used for any purpose or activity involving information subject to this Policy without prior registration of the device and written authorization by EOMC. Authorization will be given only for use of Mobile Devices which EOMC has been confirmedand configured to comply with this Policy. Authorization must be requested in writing by the department manager.
    b. Access to, obtaining, use and disclosure of information subject to this Policy by a Mobile Device, and any use of a Mobile Device in any EOMCfacility or office, including an authorized home office or remote site, must be in compliance with all EOMC policies at all times.
7. Authorization to use a Mobile Device may be suspended at any time:
    a. If the User fails or refuses to comply with this Policy.
    b. In order to avoid, prevent or mitigate the consequences of a violation of this Policy.
    c. In connection with the investigation of a possible or proven security breach, security incident, or violation of EOMC policies
    d. In order to protect individual life, health, privacy, reputational and/or financial interests.
    e. To protect any assets, information, reputational or financial interests of EOMC.
    f. Upon request of the department manager.
8. Authorization to use a Mobile Device terminates:
    a. Automatically upon the termination of a User's status as a member of the EOMC Workforce.
    b. Upon a change in the User's role as a member of the EOMC Workforce, unless continued authorization is requested by the department manager.
    c. If it is determined that the User violated this or any other EOMC policy, in accordance with EOMC policies.
    d. The use of a Mobile Device without authorization, while authorization is suspended, or after authorization has been terminated is a violation of this Policy.
9. Audit of Mobile Devices.
    a. Any Mobile Device may be subject to audit to ensure compliance with this and other EOMC policies. This includes personallyowned Mobile Devices as well as Mobile Devices owned or leased and provided by EOMC.
        i. Any User receiving such a request shall transfer possession of the Mobile Device to the IT Department at once, unless a later transfer date and time is indicated in the request, and shall not delete or modify any information subject to this Policy which is stored on the Mobile Device after receiving the request.
10. Evidentiary Access to Mobile Devices.
    a. Upon notice of a litigation hold by theIT Department or Legal Department, at their sole discretion at any time, any Mobile Device may be subject to transfer to the possession of the IT Departmentto ensure compliance with the litigation hold. Any User receiving such a notification shall transfer possession of the Mobile Device to the IT Department at once, unless a later transfer date and time is indicated in the notification, and shall not delete or modify any information subject to this Policy, which is stored on the Mobile Device after receiving the request.
11. Mobile Device User Responsibilities.
    a. In addition to other requirements and prohibitions of this and other EOMC policies, Mobile Device Users have the following responsibilities:

i. Information subject to this Policy, which is stored on the Mobile Device, must be encrypted as provided in EOMC policy. Information subject to this Policy should not be stored on the Mobile Device for any period longer than necessary for the purpose for which it is stored.
ii. A Mobile Device may not be shared at any time when unencrypted information subject to this Policy is stored on the device.
iii. A Mobile Device which does not have unencrypted information subject to this Policy stored on it may be shared temporarily, provided that:
    1. The User may not share the password or PIN used to access the Mobile Device. The User mayinput the password or PIN for an alternate user in the event shared use is required.
    2. The configuration of the device, to comply with this Policy, must not be changed.
    3. The individual using the device, not the authorized user, must not further share it; must protect it against being misplaced, lost or stolen, and must immediately report to the User if it is; and must return it promptly to the authorized user when finished with the temporary use.
    4. The individual using the device must not use it to obtain, process, use or disclose information subject to this Policy.
iv. Access to each Mobile Device must be controlled by a password or PIN number consistent with EOMC policy. Password or PINs must be changed periodically as provided in EOMC policy. The Mobile Device must provide for a maximum of 3 attempts to enter the password or PIN correctly.
v. The timeout for access to the Mobile Devices must be a maximum of 15 minutes.
vi. Information subject to this Policy which is transmitted wirelessly by the Mobile Device must be encrypted unless an exception is authorized. Exceptions must be authorized by the IT Department.
vii. If possible, Mobile Devices must have antivirus software. Mobile Devices thatcannot support antivirus software may be subject to limitations on use at the discretion of the IT Department as specified in writing by the IT Department.
viii. Physical protection for Mobile Devices must be provided as required by EOMCpolicy.
ix. Mobile devices shall not be left unattended in public areas.
x. If the Mobile Device is misplaced, stolen or believed to be compromised this must be immediately reported to theSecurity Officer.
xi. Applications and services installed on the Mobile Device must be approved by the IT Department.
xii. Bluetooth and infrared (IR) services must be configured as approved by the IT Department or turned off.
xiii. Mobile Devices must be disposed of according to EOMC policy.

12. Personal Use of Mobile Devices.
    a. Personal Use of Mobile Devices owned or leased and provided by EOMCis subject to the EOMCAcceptable Use Policy.
    b. Personal use of personallyowned Mobile Devices is not subject to the Acceptable Use Policy but must at all times be consistent with this Policy.
    c. All information on a Mobile Device, including personal information about or entered by the User, may be subject to audit or evidentiary review as provided in this Policy. Any such personal information may be used or disclosed by EOMC to the extent it deems reasonably necessary:
        i. In order to avoid, prevent or mitigate the consequences of a violation of this Policy.
        ii. In connection with the investigation of a possible or proven security breach, security incident, or violation of EOMC policies.
        iii. In order to protect the life, health, privacy, reputational or financial interests of any individual.

iv. To protect any assets, information, reputational or financial interests of EOMC.
v. For purposes of determining sanctions against the User or any other member of the EOMC Workforce.
vi. For purposes of litigation involving the User.
vii. If Required by Law.

13. Prohibited Uses of Mobile Devices.
    a. The following uses of Mobile Devices are prohibited:
        i. The storage of information subject to this Policy, including voice messages, photographs,voice notes, email, instant messages, web pages and electronic documents, images and videos, unless they are encrypted.
        ii. The Internet, wireless transmission or upload of information subject to this Policy, including voice messages, photographs,voice notes, email, instant messages, web pages and electronic documents, images and videos, without encryption, unless previously authorized in writing by the IT Department.
        iii. The creation of any photograph, image, video, voice or other recording of any individual who is a patient or member of the Workforce of EOMC, except in compliance with EOMC policy.
        iv. The creation of any photograph, image, video, voice or other recording of any document, record, computer or device screen thatincludes information subject to this Policy, except in compliance with EOMC policy.

VIOLATIONS:

Any known violations of this policy should be reported to the Security Officer. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with EOMC procedures. The EOMC may advise law enforcement agencies when a criminal offense may have been committed.