



Andrew Rexroad

Public Site CPE-125 Compliance and Ethics (Provider) 2020

Compliance



Completion

At the end of this training there is a confirmation number listed. Please record that number for verification.

Please Note

We are excited to officially transition to our new name and brand beginning January 17, 2020. As we are becoming Monument Health, you may see items (such as images, documents, policies, etc.) that say Regional Health within this training. All Regional Health branded items should be phased out by the end of the fiscal year (FY20).

Objectives

By the end of this course, learners will identify appropriate conduct when faced with compliance and/or ethical issues. During the course, learners will:

- understand the 7 elements of our Compliance Program,
- apply the Code of Conduct when faced with everyday difficult compliance/ethical decisions,

- recognize your ongoing compliance responsibilities, and
- know how to contact the Corporate Responsibility (CR) Department.

≡ A Message From Our President and CEO

≡ Corporate Responsibility

≡ Elements of an Effective Compliance Program, Policies, and Code of Conduct

≡ Auditing, Monitoring, Disciplinary Action, and Corrective Action

≡ Fraud, Waste, and Abuse

≡ Provider Relationships, EHR Compliance, and Provider Self-Disclosure

≡ Additional Topics

≡ Consent and Reportable Cases

≡ EMTALA

≡ HIPAA: Section 1

≡ HIPAA: Section 2

≡ Consequences, Non-Retaliation, and Reporting

A Message From Our President and CEO



Andrew Rexroad





Paulette Davidson, President and CEO Monument Health

Monument Health's Compliance Program was built on the foundation of integrity and serves as a reminder of our compliance responsibilities. We are

called upon to provide safe, quality care to our patients, and we achieve this by maintaining high standards.

Our organization is ultimately a reflection of each of our actions, decisions, and words. Please keep this in your mind and heart every day as you do your work.

Thank you for your continued commitment to Making a Difference. Every Day.

Best regards,

Paulette Davidson

President and CEO

Monument Health

[CONTINUE](#)

Lesson 2 of 12

Corporate Responsibility



Andrew Rexroad





Nancy Klunder, Vice President of Corporate Responsibility and Monument Health
Compliance Officer

Monument Health Compliance Officer

The Compliance Officer is responsible for implementing Monument Health's compliance program.

Corporate Responsibility reports functionally to the Compliance, Audit, and Compensation Committee and administratively to executive leadership.

Corporate Responsibility

Corporate Responsibility serves the compliance and internal audit needs of Monument Health.

The department reports directly to the Compliance, Audit, and Compensation Committee of the Monument Health Board of Trustees, allowing the team to be independent and objective.

Compliance and HIPAA

Mitigate compliance risk by maintaining a program that promotes compliance awareness, prevention, detection, and resolution of conduct that does not conform to legal or policy requirements.

Internal Audit

Mitigate business risk by providing independent review and assurance on organizational governance, risk management, and internal controls needed to achieve the strategic, operational, and financial objectives.

CONTINUE

Elements of an Effective Compliance Program, Policies, and Code of Conduct



Andrew Rexroad

Monument Health's Compliance Program is based on the **7 elements of an effective Compliance Program**, which are:

- 1 Implement written policies, procedures, and Code of Conduct
- 2 Designate a compliance officer and compliance committee
- 3 Conduct effective training and education
- 4 Develop effective lines of communication
- 5 Conduct internal monitoring and auditing
- 6 Enforce standards through well-publicized disciplinary guidelines
- 7 Respond promptly to offenses and undertake corrective action

Policy: Corporate Compliance Program

Policies and Code of Conduct

As a condition of employment and in evaluating performance, every caregiver and provider must understand and comply with Monument Health's Code of Conduct and policies.

Policies

- Compliance
- HIPAA Privacy/Security
- Internal Audit

Code of Conduct

- Guidance in upholding our ethical values and responsibilities.
- Defines acceptable behaviors to foster a culture of compliance.

If you wish to explore the contents of the Code of Conduct, please download and review the document below.



MH_Code_of_Conduct_Booklet.pdf

1.6 MB



Please click on the **button** to the right to agree to abide by the Monument Health Code of Conduct.

I AGREE

Auditing, Monitoring, Disciplinary Action, and Corrective Action



Andrew Rexroad

Auditing and Monitoring

Corporate Responsibility conducts internal monitoring and auditing.

Performed to review risk areas, determine compliance with legal requirements, and assist in the reduction of risk.

Examples of the audits conducted by the Corporate Responsibility team include:

- physician contracts
- billing and coding
- research and grant administration
- electronic health records access
- financial
- operational

Disciplinary Action

Enforce standards through well-publicized disciplinary guidelines.

Appropriate and consistent discipline of individuals who violate standards or policies will occur when warranted.

Enforcing disciplinary standards is important not only to give the Compliance Program credibility, but also to demonstrate Monument Health's integrity, commitment to compliance, and desire to prevent recurrence.

Corrective Action

Respond promptly to offenses and undertake corrective action.

For a Compliance Program to be effective, all allegations are evaluated and investigated.

Non-compliant conduct will be immediately addressed and the effects of non-compliance will be mitigated.

The goal of any corrective action is to address non-compliance and reduce the likelihood of recurrence.

CONTINUE

Fraud, Waste, and Abuse



Andrew Rexroad

The presence of some dishonest health care providers who exploit the health care system for illegal personal gain has created the need for laws that combat fraud and abuse, along with ensuring appropriate quality medical care. Following are the laws:

False Claim Act

It is illegal to submit claims for payment to Medicare or Medicaid you know or should know are false or fraudulent.

Anti-Kickback Statute

It is a felony to knowingly or willfully offer, pay, solicit, or receive any payment for referrals of items or services reimbursable by a Federal health care program.

Physician Self-Referral Law (Stark Law)

The Stark law is a strict liability statute, which means proof of specific intent to violate the law is not required. The Stark law prohibits a physician from making a referral for certain designated health services to an entity in which the physician (or an immediate member of his or her family) has a financial relationship with, unless an exception applies.

Civil Monetary Penalties Law

The Government may seek civil penalties for a wide variety of conduct and is authorized to seek different amounts of penalties based on the type of violation. Penalties range from \$10,000 to \$50,000 per violation.

Some examples of violations include:

- Presenting a claim the person knows or should know is for an item or service not provided as claimed or is false or fraudulent.
- Presenting a claim the person knows or should know is for an item or service for which payment may not be made.
- Providing false or misleading information expected to influence a decision to discharge.
- Failing to provide an adequate medical screening examination for patients who present to a hospital emergency department with an emergency medical condition or are in labor.
- Making false statements or misrepresentations on applications or contracts to participate in Federal health care programs.

Avoiding Fraud, Waste, and Abuse

- Accurate coding and billing
 - correct codes for services provided
- Documentation compliance
 - complete and accurate
 - represents reasonable and necessary services
 - includes signature, date, and time
 - signatures that cannot be read include the printed name

Do not create or participate in the creation of any records intended to mislead or conceal anything improper.

Once you become enrolled as a Medicare and/or Medicaid provider, you are responsible for ensuring claims submitted under your number are true and accurate.

Any time a health care business offers something to you for free or at below fair market value, you always should ask yourself “*Why*” because it could put you at risk.

Provider Investments in Health Care Business Ventures

If you are invited to invest in a health care business whose products you might order or to which you might refer your patients, you should consider carefully whether you are investing for legitimate reasons.

Ask yourself the following questions:

- Are you being offered an investment interest for a nominal capital contribution?
- Will your ownership share be larger than your share of the aggregate capital contributions made to the venture?
- Is the venture promising you high rates of return for little or no financial risk?
- Is the venture or any potential business partner offering to loan you the money to make your capital contribution?
- Are you being asked to promise or guarantee that you will refer patients or order items or services from the venture?
- Do you believe you will be more likely to refer more patients for the items and services provided by the venture if you make the investment?
- Do you believe you will be more likely to refer to the venture just because you made the investment?
- Will the venture have sufficient capital from other sources to fund its ongoing operations?

CONTINUE

Provider Relationships, EHR Compliance, and Provider Self-Disclosure



Andrew Rexroad

Transparency in Provider Relationships

The Patient Protection and Affordable Care Act requires drug, device, and biologic companies to publicly report nearly all gifts or payments they make to providers.

Academic institutions also may impose various restrictions on the interactions their faculty members or affiliated providers have with industry. These and other considerations may factor into your decision about whether you want to conduct industry-sponsored research; serve as a consultant or director for a drug, biologic, or device company; apply for industry-sponsored educational or research grants; or engage in other relationships with industry.

Both the pharmaceutical industry (through PhRMA) and the medical device industry (through AdvaMed) have adopted codes of ethics for their respective industries regarding relationships with health care professionals. Both codes are available online.

Electronic Health Record (EHR)

CMS and the OIG are reviewing records for:

- **Cut & Paste:** Blocks of text or even complete notes from another provider or previous appointment.
- **Copy & Paste:** Duplication from a prior note to a new note.
- **Other terms used:**

- cloning
- copy forward
- re-use
- carry forward

Make appropriate changes to documentation!

Compliance Department recommendations:

- documentation for each encounter must be specific to:
 - date of service
 - patient problem
- only allow PFSH, ROS, allergies and/or medications to auto-flow into a new encounter
 - verify accuracy
 - update with current date of service

Potential Problem?

If you think there is a problem or you have been following billing practices you now think were wrong which impacts Monument Health:

- immediately cease the problematic conduct
- contact the Compliance or Legal department

Overpayments will be returned or reported, as appropriate.

Provider Self-Disclosure

There is a Self-Disclosure Protocol for providers to voluntarily disclose self-discovered evidence of potential fraud.

The protocol allows providers to work with the government to avoid costs and disruptions during a government-directed investigation.

For more information on this Self-Disclosure Protocol, contact the Compliance or Legal department.

CONTINUE

Additional Topics



Andrew Rexroad

Exclusion Statute

Under the **Exclusion Statute**, the Office of Inspector General (OIG) is required to impose exclusions from participation in all Federal health care programs on health care providers and suppliers who have been convicted of:

- Medicare or Medicaid fraud
- patient abuse or neglect
- felony convictions for health care-related fraud, theft, or other financial misconduct
- felony convictions for unlawful manufacture, distribution, prescription, or dispensing of controlled substances

Excluded providers may not receive Medicare payment.

Conflict of Interest

A potential conflict of interest exists when you or a member of your family works for or has a financial relationship with a company:

- doing business with Monument Health (MH)
- seeking to do business with MH
- competing with MH

These types of relationships should be reported to Legal Services or Corporate Responsibility.

Drug Free Workplace and Drug Diversion

The Drug Free Workplace/Drug Diversion policy accomplishes two major things:

- Sends a clear message alcohol and drug use and drug diversion in the workplace is prohibited.
- Encourages providers and caregivers who have problems with alcohol and other drugs to voluntarily seek help.

Provider and caregiver responsibilities:

- Do not enable others, cover-up, or make excuses for others when there is suspected abuse or diversion.
- Express concern and encourage the individual to seek help.
 - Guidance Resources Employee Assistance Program (EAP)
- Report suspected drug diversion/abuse to their director or supervisor.

Signs that a healthcare professional may be diverting drugs:

- always volunteers to give medications
- patients complain of no pain relief from medications documented as given
- discrepancies on medication administration records
- has frequent wastage, such as spilling drugs or breaking vials
- narcotics signed off controlled substance record but not recorded on patient report

Policy: Drug Free Workplace and Drug Diversion Guidelines

Gifts

Per policy, nominal gifts (under a \$25 value) may be accepted.

- Never accept gifts from patients while they are inpatient.
- Never accept cash or cash equivalents from patients or family members.
- If a patient or family member mentions wanting to give a gift, politely decline. If they persist, mention they could make a donation to the foundation or give a modest gift to share with the department, such as bagels.
- If a patient or family shows up with a gift, thank them on behalf of the department and report to your supervisor.
- Gifts over \$25 may be subject to tax.
- Review the Gifts, Gratuities, and Entertainment policy for more information regarding gifts from patients, vendors, etc.

Hallway Medicine

Approaching a provider at work for free medical advice may seem harmless, but has concerning complexities. Think of it as a free clinic visit; you would have had to make an appointment in order to obtain that care.

Free care is prohibited by Monument Health policy unless a patient qualifies under our Financial Assistance Program.

We respectfully request caregiver and provider cooperation in refraining from requesting or providing free medical care.

CONTINUE

Consent and Reportable Cases



Andrew Rexroad

Consent

We must have patient permission before we provide treatment.

We should discuss the nature of the treatment, as well as the risks, benefits, and alternatives of the treatment.

- Adults (over the age of 18) who have the capacity to make their own medical decisions may provide consent for their own treatment.
- Adults who do not have capacity to make their own medical decisions may use a surrogate decision-maker to provide consent.

South Dakota Law recognizes the following hierarchy for surrogate decision-makers:

- 1 Court appointed guardian;
 - 2 Designated Durable Health Care Power of Attorney;
 - 3 Spouse, if not legally separated;
 - 4 Adult child;
- 

- 5 Parent;
- 6 Adult Sibling;
- 7 Grandparent or adult grandchild;
- 8 Adult aunt, uncle, cousin, niece or nephew; and
- 9 Close friend.

- Minors (under the age of 18) - consent to treat must be given by the parent, guardian or legal custodian, e.g. Department of Social Services (DSS).
 - **Exception - the diagnosis and treatment of sexually transmitted diseases for anyone under the age of 18 does not require parental consent and should be kept confidential.**
- Consent must be documented in the medical record.

Reportable Cases

Certain events require a mandatory report to law enforcement:

- gunshot wounds, bullet wounds, powder burns, or any injury inflicted by the discharge of a firearm;
- abuse or neglect of a minor;
- animal bites or scratches (as required by relevant city ordinance);
- suspected felony committed against a patient in our healing environment;
- abuse, neglect, or exploitation of elders or disabled adults; and
- any reasonable suspicion of a crime committed against a resident of a long-term care environment.

CONTINUE

EMTALA



Andrew Rexroad

Emergency Medical Treatment and Active Labor Act (EMTALA)

EMTALA prohibits a hospital from delaying care, refusing treatment, or transferring patients to another hospital based on the patient's inability to pay for services.

If an individual presents to a hospital's emergency department, the hospital must:

- Provide an appropriate medical screening examination within the capability of the hospital's emergency department to determine whether or not an emergency medical condition exists.
- The examination must be conducted by an individual(s) determined to be qualified by hospital bylaws or rules and regulations.
- If an emergency medical condition is determined to exist, provide any necessary stabilizing treatment or an appropriate transfer.
- If the hospital admits the individual as an inpatient for further treatment, the hospital's obligation under EMTALA ends.

EMTALA applies to hospitals with a dedicated emergency department, including:

- any department of that hospital
- any part of that hospital campus (defined as):
 - hospital buildings adjacent to the main buildings
 - parking lot, sidewalk, and driveway
 - hospital buildings within 250 yards of the main buildings (whether or not contiguous)

Consider the following example:

A patient with chest pain presents to a hospital-owned clinic 100 yards from the hospital, which has a dedicated Emergency Department.

- Does the hospital have an EMTALA obligation for the care of this patient?

Answer:

Yes, the clinic meets the definition of *hospital campus*, thus the clinic has an EMTALA obligation.

“Medical Screening Examination”

Evaluation to determine whether an emergency medical condition exists, which is the same as or similar to the screening provided to all patients presenting to the emergency department complaining of the same condition or exhibiting the same symptoms.

The key take-away is to evaluate each encounter in an objective manner without prejudice of previous encounters with patient.

“Medical Screening Examination” must be:

- provided to every presenting patient without undue delay
- sufficient in scope to determine whether an emergency condition exists
- conducted by a credentialed provider

Obtaining registration and/or payment information must not delay the Medical Screening Exam.

“Capacity”

The ability of the hospital to accommodate the individual requesting examination or treatment of the transferred individual.

Capacity encompasses such things as numbers and availability of qualified staff, beds, equipment, and the hospital's past practices of accommodating additional patients in excess of its occupancy limits.

Consider the following example:

The Emergency Department receives a call from a referring hospital requesting to transfer a patient for surgical services. There are only four available beds. The Emergency Department has been extremely busy and they are anticipating additional admissions during the night.

- Is it acceptable to deny the transfer?

Answer:

No, the transfer must be accepted if there is *capacity* at the time of the request for transfer.

- It is not acceptable to “hold” beds for potential future admissions.

“Emergency Medical Condition”

Acute symptoms of sufficient severity (including severe pain, psychiatric disturbances and/or symptoms of substance abuse) where the absence of immediate medical attention could reasonably be expected to result in placing the health of the individual in serious jeopardy, such as:

- serious impairment to bodily functions;
- serious dysfunction of any bodily organ or part; or

- a pregnant woman who is having contractions:
 - inadequate time to effect a safe transfer to another hospital before delivery; or
 - transfer may pose a threat to the health or safety of the woman or the unborn child.

Consider the following example:

A patient presents to the Emergency Department with a complex ankle fracture deemed by the Emergency Department provider to need surgery. The orthopedic surgeon on-call and partner are in emergency surgery with 4 cases pending.

- Is it acceptable to divert the patient?

Answer:

Yes, it is acceptable.

- While this is an *emergency medical condition*, the on-call providers are unavailable due to emergency surgery, thus the hospital does not have the *capacity* to treat the individual.

Against Medical Advice

CMS clarified EMTALA obligations exist for hospitals even when a patient leaves without notifying the hospital.

For any patient who refuses further care or “leaves without being seen,” the emergency department staff must log, document, and retain:

- who refused care
- what time the hospital discovered the patient left

- all triage notes and additional records

If investigated by CMS, the hospital must show the refusal of care was not due to delay of care caused by discriminatory reasons, such as insurance status, race, color, nationality, gender, etc.

DOCUMENT, DOCUMENT, DOCUMENT.

EMTALA obligations end when the patient is “stable.”

A patient is deemed stabilized if the attending provider has determined, with reasonable clinical confidence, the emergency condition has resolved.

A patient is considered stable for discharge when a provider determines, with reasonable clinical confidence, the patient has reached the point where continued care, including diagnostic workup and/or treatment, could reasonably be performed on an outpatient basis.

On-call Responsibility

As a requirement for participation in the Medicare program, hospitals must maintain a list of providers who are on-call.

The emergency department provider has the ultimate authority in deciding whether the specialist needs to come to the hospital to help stabilize the patient.

If the on-call provider refuses to come to the hospital and the emergency provider is forced to transfer the patient for emergency care, EMTALA mandates the name and phone number of the refusing on-call provider be documented on the chart so the receiving hospital can report the on-call provider.



On-call Responsibility

On-call providers need to fully understand their EMTALA responsibilities.

On-call providers must respond to the hospital when requested to attend to patients in-person in a timely manner and complete a Medical Screening Exam or provide stabilizing care **unless circumstances beyond the provider's control** prevent a response.



Prior to transfer, a patient must be stabilized to the best of the hospital's capability.

Once the transfer is determined to be necessary, the transferring provider must speak directly to the receiving provider and obtain acceptance.

- Documented on the certificate of transfer.

Additionally, the medical benefits associated with the transfer should outweigh the risks and must be documented on the certificate.

Patients must be transferred using appropriate means of transportation, equipment, and personnel.

If the patient refuses ambulance transfer, and chooses to go in a private vehicle, an "AMA form" must be completed. This form provides documentation of events should questions arise after the patient

leaves.

When a hospital's resources are at capacity and converts to diversionary status, it is not required to accept further transfers.

The following must be documented:

- **date**
- **time**
- **reason**

EMTALA Violations

- A hospital can be fined between \$25,000 - \$50,000 per violation.
- Hospitals can be excluded from the Medicare program.
- Providers can be fined up to \$50,000 per violation.
- Providers can be excluded from Medicare/Medicaid.

CONTINUE

HIPAA: Section 1



Andrew Rexroad

Identity Theft: Red Flags

“Red Flags” are patterns, practices, or activity indicating the possible existence of identity theft.

If identity theft or any patient misidentification is suspected, immediately notify your leader.

Examples of “Red Flags”:

- Records are inconsistent with the physical state of the patient or his/her medical history.
- Records show substantial discrepancies in age, race, sex, or other physical description.
- Documents appear to be forged or altered.
- The photograph doesn't match the patient.
- The patient cannot readily validate the ID information on file.

All registration/intake areas of Monument Health shall review and include in each patient's file a copy of a photo ID issued by a local, state, or federal government agency (e.g. driver's license, passport, military ID, etc.).

**If suspicious activity is identified in the Emergency
Department, do not delay care!**

Policy: Identity Theft Program

What is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA).

What does HIPAA do?

- Requires Monument Health to protect and secure our patients' Protected Health Information (PHI).
- Defines how patient information can be used and disclosed.
- Gives patients privacy rights and more control over their own health information.
- Specifies a series of safeguards to assure the confidentiality, integrity, and availability of electronic PHI (e-PHI).
- Requires notification, if warranted, to individuals when their PHI is breached.

HIPAA – Patient Privacy Rights

HIPAA provides patients with specific rights related to their PHI:

- request restriction of uses and disclosures
- request alternative forms of communications
 - mail to P.O. Box, not street address
- obtain a copy of their record
- request an accounting of disclosures of PHI
- request amendments to their information

Policies are in place to ensure each of these rights are upheld and respected.

HIPAA – Protected Health Information

What is PHI?

Any information which can be:

- linked to a specific patient, directly or indirectly
- created or received by a covered entity
- pertains to a patient's past, present, and/or future treatment and payment
- information sent or stored in any form:
 - **verbal** discussions
 - **written** on paper
 - **electronic**
 - computer applications and systems
 - computer hardware/equipment

HIPAA - PHI

18 PHI identifiers:

- Name
- Address
- Dates
- Phone number
- Fax number
- Email address
- URL address
- IP address
- Social Security number
- Account number
- License number
- Medical record number
- Health plan beneficiary number
- Lab results
- Images
- Biometric identifiers
 - Fingerprint, hand print, etc.
- Full face photos
- Any unique identifiable number, characteristic, or code



18 PHI identifiers

HIPAA – Permitted Uses and Disclosures

When can you access, use, or share PHI without written authorization from the patient?

- Treatment (discussions among providers, sending medical records to primary care providers, etc.)
- Payment (billing and collecting activities, review for medical necessity, etc.)
- Operations (quality assessments, audits, training/education purposes, peer review, etc.)
- Exceptions allowed under HIPAA, for example:
 - court orders

- public health activities
- reporting abuse, neglect or domestic violence
- Worker's Compensation
- certain law enforcement activities

Policy: HIPAA Privacy – Uses and Disclosures Not Requiring Patient Authorization

HIPAA permits PHI to be shared with law enforcement under limited circumstances:

- 1 In an attempt to identify or locate a suspect, fugitive, material witness, or missing person. *Only specific information is allowed to be disclosed. Review policy prior to releasing information.*
- 2 The patient is a victim of a crime, and is: **Alert and cognizant** – *obtain patient consent to disclose PHI and document this in the medical record*; **Unable to consent** – *note this in the medical record.*
- 3 When there is a crime on Monument Health property. *The PHI sought by law enforcement is evidence of a possible crime on MH property.*
- 4 When the patient is in lawful custody. *The officer must maintain custody of the patient during treatment.*

If an officer drops off a patient and requests to be called when the patient is to be discharged, is it okay to call? **NO**

****Law enforcement **must complete** the "Request from Law Enforcement for Release of Protected Health Information" prior to releasing PHI.**

Policy: HIPAA Privacy – Guidance on Disclosing PHI to Law Enforcement or as Required by Law

HIPAA – Incidental Disclosures

“Incidental” means a use or disclosure that cannot reasonably be prevented, is limited in nature, and occurs as a by-product of an otherwise permitted use or disclosure.

Examples:

- Communicate and coordinate services at hospital nursing stations.
- Discuss a patient’s condition quietly in a semi-private room or a waiting room.
- Discuss a patient’s condition during teaching rounds.
- Discuss a prescription with a patient over the pharmacy counter.

Incidental uses and disclosures are permitted, so long as reasonable safeguards are used to protect PHI and minimum necessary standards are applied.

- Speak in lower tone of voice.
- Take the conversation to a private location, if possible.

In emergency situations, loud emergency rooms, or where a patient is hearing impaired, precautions may not be practical. In these cases, health care staff are free to engage in communications as required to provide quick, effective, and high quality care.

HIPAA – Disclosures to Family and Friends

A patient’s health information may be verbally disclosed to family, friends, or others involved in the patient’s care according to the following guidelines:

- **Patient is present, alert, and capable of making decisions:**
 - give the patient the opportunity to object; obtain verbal agreement

- infer from circumstances that the patient does not object
 - Example: Patient asks to have their spouse or friend present in the examination room.

- **Emergency or incapacitated patients:**

- refer to the “Guidelines on Patient's Lacking Decision Making Capacity and Surrogate” policy
- use professional judgment to determine whether the disclosure is in the best interest of the patient and, if so, disclose only the information directly relevant to the person's involvement with the patient's health care or related payment
- as soon as reasonably possible, the patient will be given the opportunity to agree or object to this practice

Policy: HIPAA Privacy - Disclosure of PHI to Family and Others Involved in Patient's Care

CONTINUE

HIPAA: Section 2



Andrew Rexroad

HIPAA – Valid Authorizations



Authorization for Disclosure/Release of Protected Health Information

Providers may not otherwise access or disclose PHI unless the patient has given written authorization.

This form can be found on the Intranet under the Forms page or Corporate Responsibility Hub page.

Policy: HIPAA Privacy – Uses and Disclosures Requiring Patient Authorization and Authorization Requirements

HIPAA - Minimum Necessary and Need to Know

When is it appropriate to:

- view PHI
- use PHI
- share PHI

Only when required for your job!

You must also only access, use, or share the “**minimum necessary**” amount of PHI you need to do your job.

Policy: HIPAA Privacy – Handling Confidential Information, Reporting Violations and Use of Confidentiality Agreement

HIPAA – Patient Privacy Rights

Directory Disclosures:

Patients have the right to restrict the release of their directory information.

- Unless the patient objects, the following PHI may be included in the hospital directory and given to those individuals who inquire about the patient by name:
 - name
 - location within the hospital
 - condition of the patient in general terms (e.g., good, critical, serious)
 - only members of the clergy may have access to the religious affiliation of the patient, if provided
- If the patient has opted out of the patient directory:

- Any member of the public seeking information on the location of a patient should be directed to or transferred to the hospital's Guest Service desk or communication center to ensure the patient's directory wishes are upheld.
- Their information will not be disclosed to any member of the public, including family, friends, florists, clergy, etc.

Policy: HIPAA Privacy – Patient Directory Guidelines

HIPAA Security – Safeguards

Email Security:

Use secure email when emailing PHI or other business sensitive information outside of Monument Health. **Do not** use your personal email (Yahoo, Gmail, Hotmail) to send/receive PHI!

- Include "SecureMail" in the subject line.



Email security

Policy: Information Security – Acceptable Use of Information Technology Resources

HIPAA – Protecting PHI

Paper

- Immediately gather documents you sent to a printer. Use “Secure Print” to avoid documents sitting on the printer.
- Turn documents over that contain PHI when in the presence of another person.
- **Double check** when mailing or handing out documents; verify **each page** belongs to that patient.

Verbal

- Be aware of your surroundings; do not discuss PHI in public areas such as elevators or the cafeteria.
- Do not leave details, such as test results or treatment plans in a voicemail.
 - Message can include your name, healing environment name, and phone number to call back.
 - If the healing environment name identifies type of care, such as Cancer Care Institute, state “Monument Health.”

Policy: HIPAA Privacy – Handling Confidential Information, Reporting Violations and Use of Confidentiality Agreement

Social Media

- Do not share any patient information learned through work on social media.
- Posting patient information without authorization is a violation of the patient’s right to privacy and confidentiality.
- Even if you think you’ve de-identified the information (removed all 18 identifiers), depending on the situation it still might be identifiable to others.

Policy: Social Media

Electronic PHI

Email

- Double check email addresses and attachments before sending PHI to ensure the information is sent to the correct recipient; remember to send securely.

Texting/Messaging Apps

- Use of standard texting/messaging apps to send PHI is not permitted as it is not secure or encrypted; only Monument Health approved and secure apps, such as Haiku, Canto, and Rover may be used.
- Contact the IT Help Desk if you have questions about other secure texting/messaging that may be available.

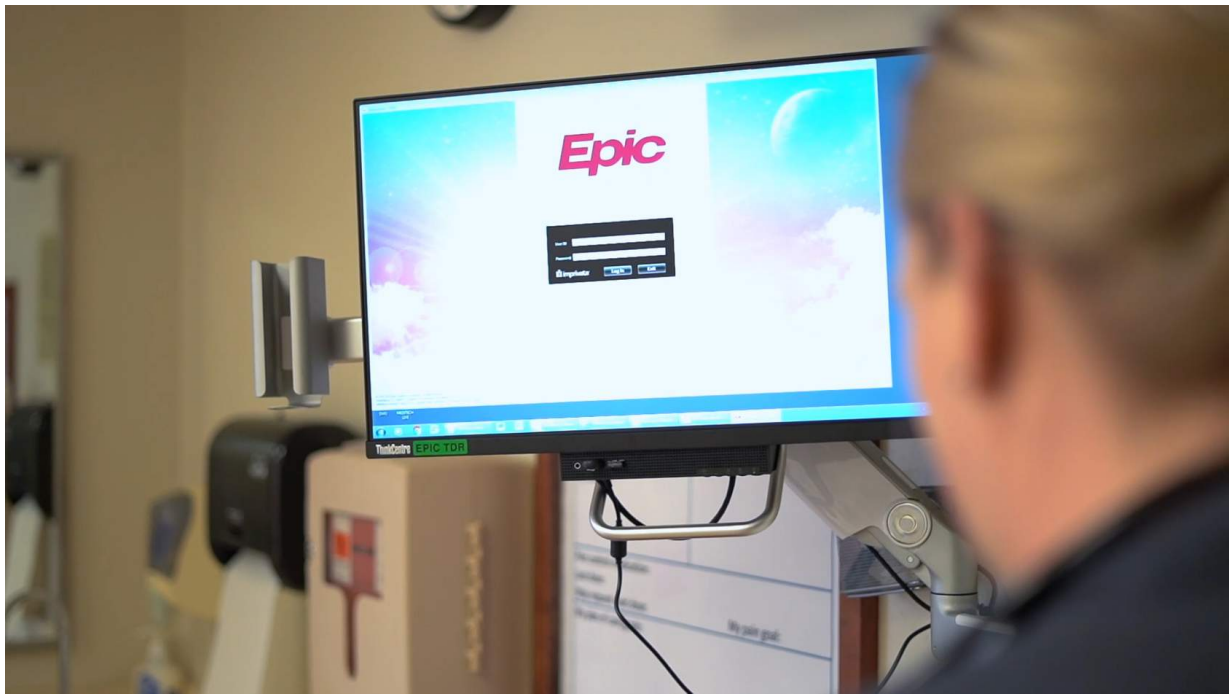
Fax

- Double check the fax number before sending PHI to ensure the information is sent to the correct recipient.

Patient Photos/Videos

- Taking photographs or videos of patients with personal mobile devices, outside a secure app, is prohibited.
- In situations where photographs are necessary:
 - Use a Monument Health device
 - Use a personal device only when logged into a secure, Monument Health approved app, such as Haiku, Canto, and Rover, because no data/photos are physically stored on the device (smart phone, iPad, iPod, etc.)

Policy: Information Security – Acceptable Use of Information Technology Resources



Epic

Electronic Medical Record (EMR)

Access

- **Do not** access a patient record out of curiosity (no snooping).
- **Do not** access your own record or the records for your children or other family members.
- **Do not** access the records of friends or co-workers.
- **Do not** access records under another user's login.

If you do **not** have a legitimate business purpose (necessary to perform your job function) for accessing a patient's PHI, you are **not** allowed to view that information.

Audits are conducted to ensure appropriate access. If inappropriate access is identified, disciplinary action will be taken.

Policy: HIPAA Privacy – Handling Confidential Information, Reporting Violations and Use of Confidentiality Agreement

HIPAA – Disposal of PHI

Disposal of PHI

- Never dispose of paper or other items containing PHI in the regular trash.
- All paper should be disposed of in the shred bins.
- Non-paper items should be destroyed in the appropriate manner according to your healing environment's process.
- CDs, thumb drives, computers, etc. containing PHI should be sent to the IT Help Desk for appropriate disposal.

Policy: Disposal of Confidential Information

HIPAA – Breaches

By law, a breach occurs when protected health information is:

- **lost, stolen, or improperly disposed of**
 - paper or device upon which the information is recorded cannot be accounted for
- **“hacked”** into by people or mechanized programs not authorized to have access
 - the system in which the information is located is compromised
- **communicated or sent** to others who have no official need to receive it
 - medical record is faxed/emailed/mailed to the wrong individual
 - posting patient information to social media

Examples of HIPAA breaches:

- Placing PHI in the trash bin.
- Scanning EHR for potential patients.
- At the request of a friend or family member, accessing the record without a treatment relationship established.
- Entering the wrong ordering/family/attending provider; the report is faxed to the wrong provider.
- Communicating with another provider or caregiver about a patient using a personal, unsecure texting app.

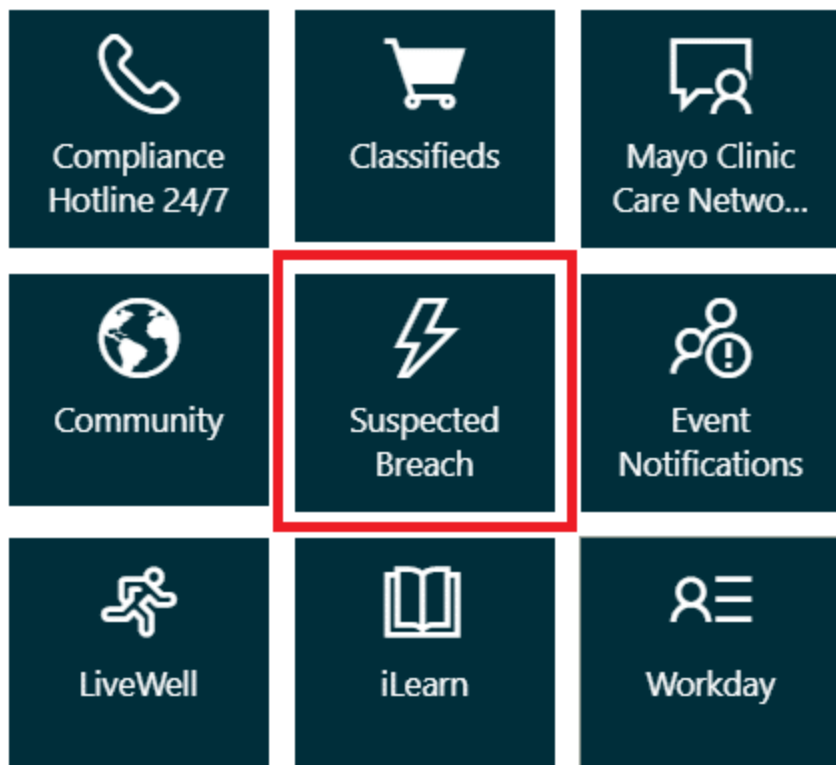
HIPAA – Report Breaches

Part of your responsibility as a Monument Health caregiver is to report privacy or security breaches involving PHI.

Example: Patient calls and states she received another patient’s statement. What do you do?

- **Action:** Ask the recipient to shred or return the information.

Helpful Links



Helpful Links - Suspected Breach

Report: Inform your leader of the breach.

- Complete and submit the "Suspected Breach of Health Information" form to Corporate Responsibility. The form can be found on the Intranet under "Helpful Links." Click on the **Suspected Breach icon**.
- **Timeframe:** Report any issues and suspected privacy/security violations immediately.

Any impermissible use or disclosure may trigger breach notification requirements to the patient and the federal government.

Policy: HIPAA Privacy – Compliance with the Breach Notification Rule

CONTINUE

Consequences, Non-Retaliation, and Reporting



Andrew Rexroad

HIPAA – Consequences of Non-Compliance

Sanctions. Workforce members using PHI inappropriately will be subject to disciplinary action (based on the severity of the violation), which may include:

- **education**
- **written warning**
- **termination**

Penalties. The Department of Health and Human Services (DHHS), Office for Civil Rights (OCR) is responsible for administering and enforcing the HIPAA standards. They may conduct investigations and reviews to determine compliance with HIPAA and may impose **Civil Monetary Penalties** for both the individual and the organization.

Non-Retaliation

Monument Health is committed to protecting those who report problems and concerns in good faith from retaliation, retribution, harassment, intimidation, threats, and/or verbal abuse.

- No disciplinary action or retaliation will be taken against you when you report a perceived issue, problem, concern, or violation “in good faith.”

- “In good faith” means you actually believe the information reported is true.
- Retaliation will not be tolerated.
- The Non-Retaliation policy is in place to reassure those who report concerns are protected from retaliation.

Reporting Options

Compliance is everyone’s responsibility!

We all have a duty to report Compliance/HIPAA issues!

You are encouraged to use the following options to resolve any questions or concerns you may have:

- Discuss the question or concern with your direct leader. Give your leader a chance to solve the problem. He/she is most familiar with the laws, regulations, and policies that relate to your work.
- If you are not comfortable talking to your leader or feel you did not receive an adequate response, contact your leader’s manager, another member of the management team, or physician leadership.
- Contact the Human Resources (HR) office or your HR Business Partner at 755-5510.
- Contact Corporate Responsibility at 755-9020.
- Report anonymously (if requested) through the Compliance Hotline.
 - Call 877-800-6907
 - Submit electronically via the link on the Intranet

Home Caregiver Hub Business Hub Clinical Hub Facilities

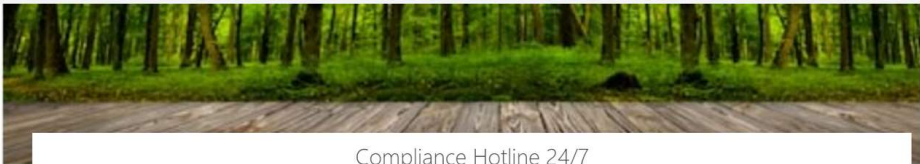
CR Corporate Responsibility Hub
Home Documents Site Directory

☆ Not following

Search this site

Send by email

Published 12/24/2019



Compliance Hotline 24/7

Call 877-800-6907 to speak to a specialist who will help you document your report.

[Click to submit your report online](#)

Corporate Responsibility Hub Compliance Hotline (Intranet)

Reporting Concerns

What Should Be Reported?

- Illegal acts
- Violations of our Code of Conduct
- Patient privacy concerns
- Policy violations
- Provider misconduct
- Quality and safety concerns
- Fraud and falsification of documentation
- Inaccurate billing
- Research misconduct
- Conflicts of Interest
- Misuse of company assets/property
- Retaliation/harassment

What Should NOT Be Reported to the Hotline?

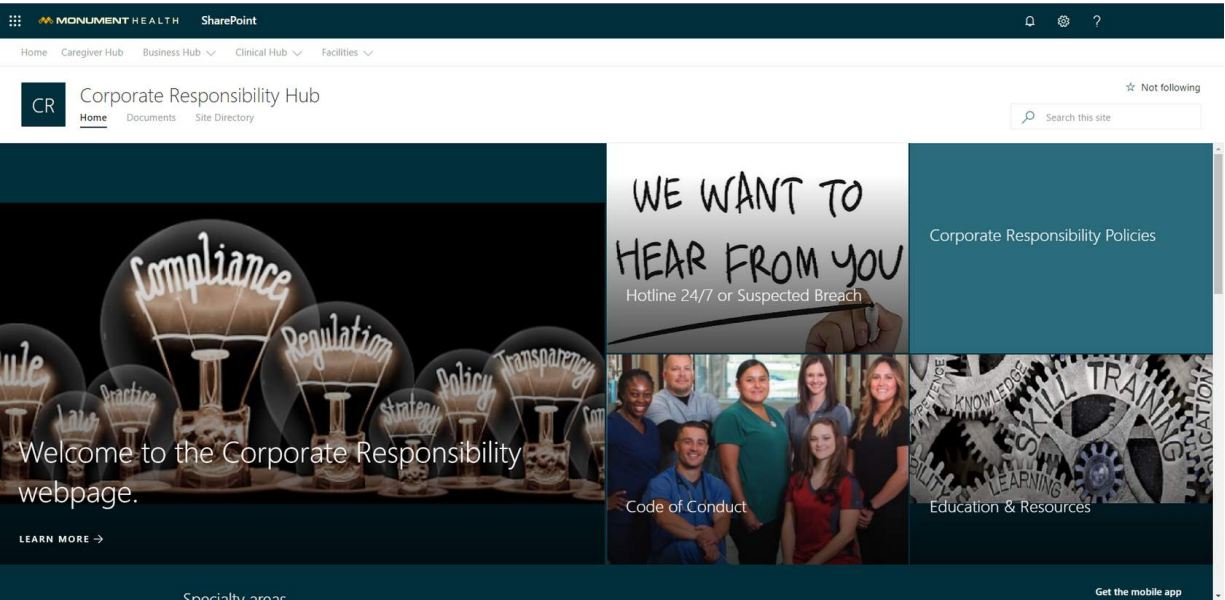
- Emergencies (Call 911)
- Employment concerns should be addressed with HR at 755-5510
 - Performance evaluations
 - Pay raises
 - Supervisory issues
- IT issues call the IT Help Desk at 755-8131

Reporting Concerns, What should be reported? What should NOT be reported to the Hotline?

Corporate Responsibility Hub Page

Visit the Corporate Responsibility hub page on the Intranet for more information!

Intranet Home Page – Facilities – Corp Svcs then click Corporate Responsibility Hub on left menu.



Corporate Responsibility Hub Page

Please record the following number for completion: 786314.

