Public Site CPE-130 Compliance and Ethics (Contractor/Vendor) 2020

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

Additional Topics

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 9

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 & 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. Written policies, procedures, and a Code of Conduct
2. A Compliance Officer that is accountable and responsible for the program
3. Effective training and education
4. Lines of communication for reporting compliance concerns
5. Disciplinary action for non-compliance
6. Routine monitoring and auditing to identify risks
7. Procedures for responding promptly to non-compliance and undertaking 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

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.

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.

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.

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.

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 abuse to your leader.

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.

Policy: Gifts, Gratuities, and Entertainment

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

HIPAA: Section 1

Andrew Rexroad

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 – 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 – 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

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 interests 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

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 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.

CONTINUE

HIPAA: Section 2

Andrew Rexroad

HIPAA – Facility Directory

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 - Minimum Necessary and Need to Know

When is it appropriate to:

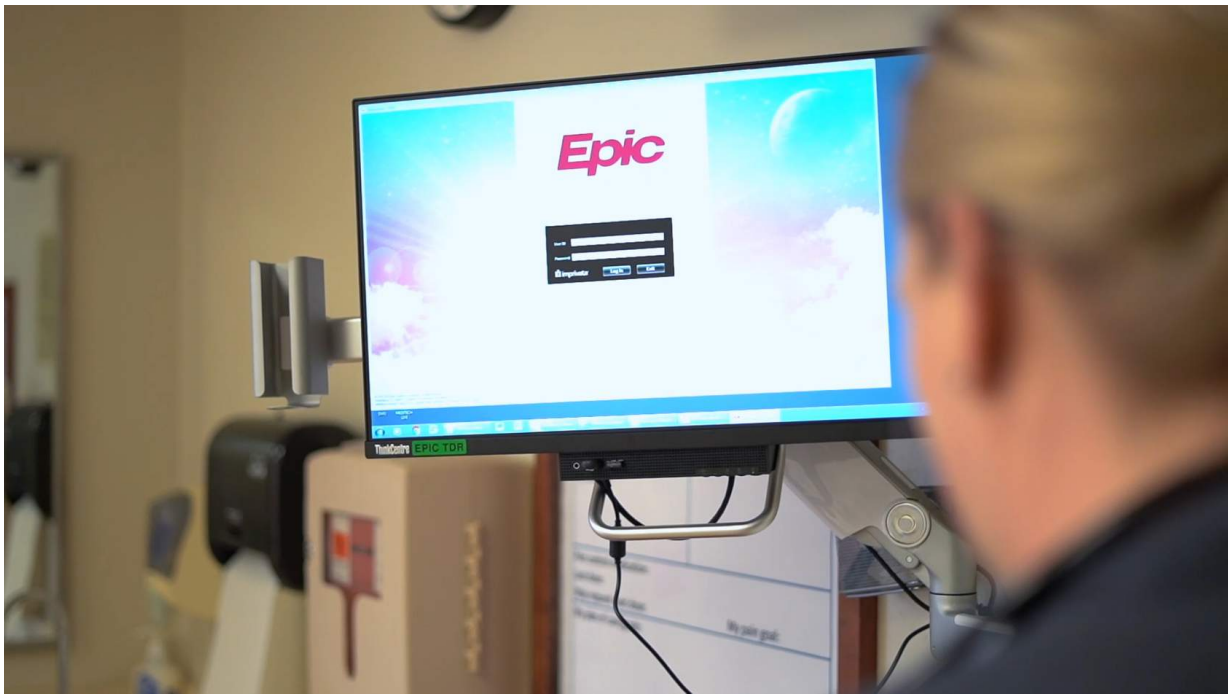
- **view PHI**
- **use PHI**
- **share PHI**

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 – Protecting PHI



Epic

If you have access to the Monument Health Electronic Medical Record (EMR) Epic system:

- **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 – 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

HIPAA – Breaches

A breach occurs when information, by law, must be protected 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

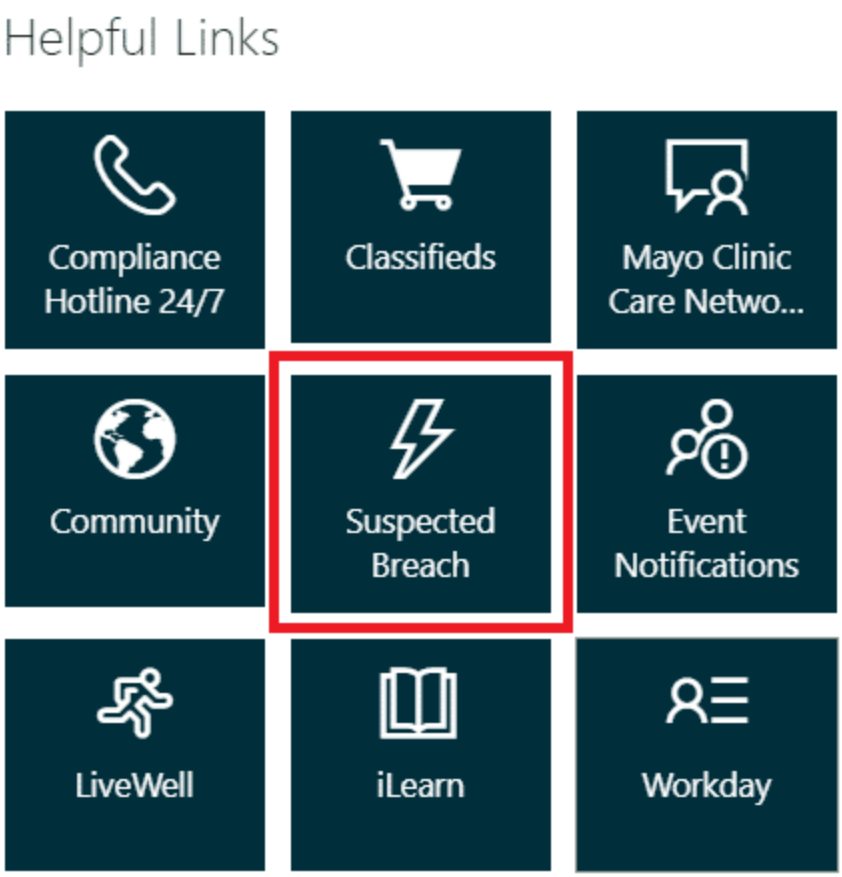
- **communicated or sent** to others who have no official need to receive it
    - medical record is faxed/emailed/mailed to the wrong individual
    - posting patient information to social media

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 in the mail. What do you do?

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



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 unauthorized 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.

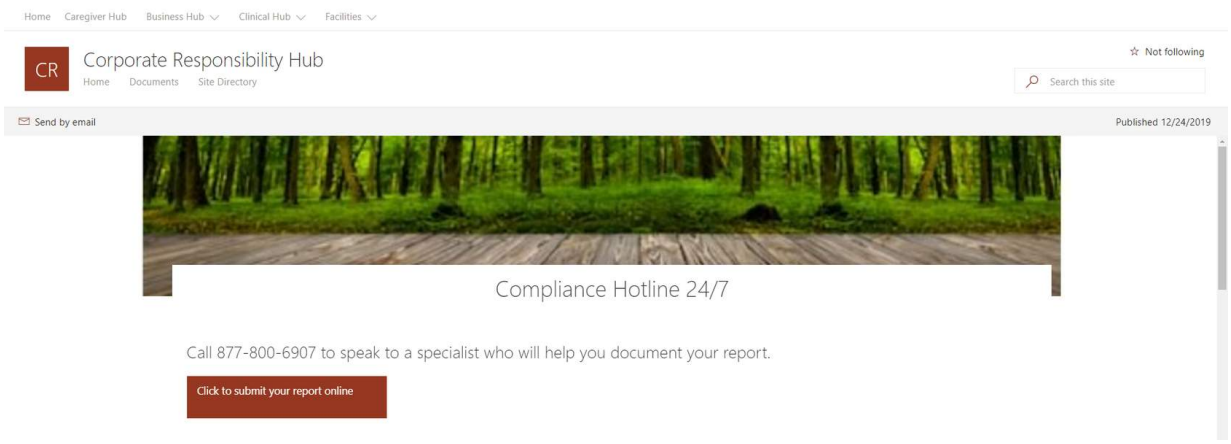
Reporting Options

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 supervisor. Give your supervisor 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 supervisor or feel you did not receive an adequate response, contact your supervisor’s manager or another member of the management team.
- 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



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?

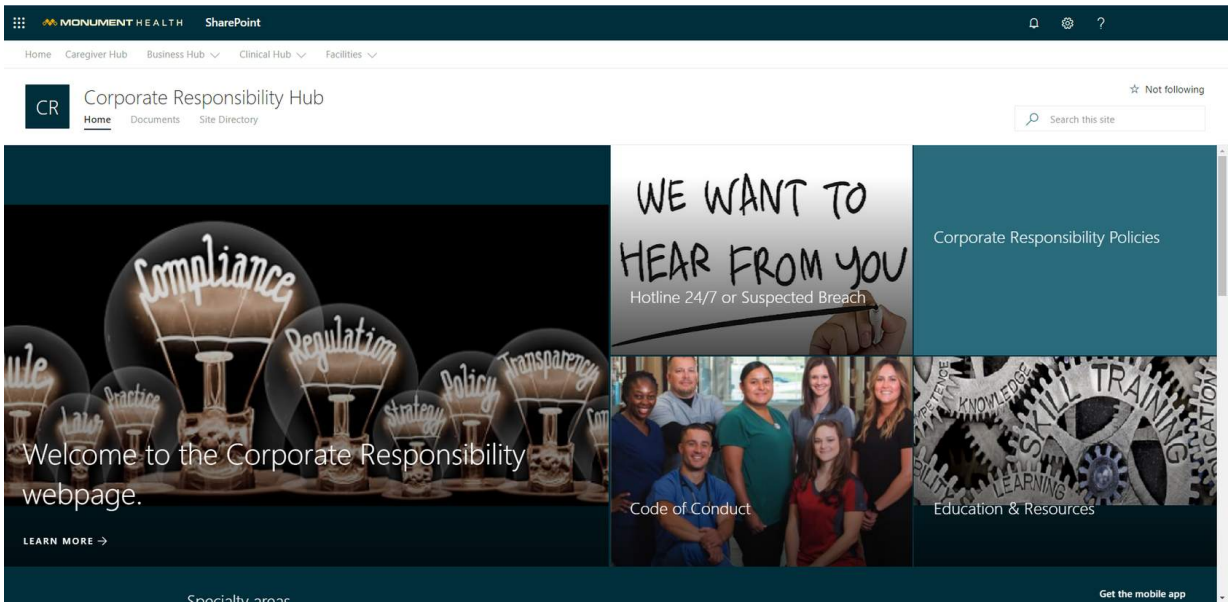
- Emergencies (Call 911)
- Employment concerns should be addressed with HR at 755-5510
  - Performance evaluations
  - Pay raises
  - Supervisory issues
- IT issues call the IT Help Desk at 755-8131

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: 147953.

CONTINUE