Regional Health

Compliance & Ethics Training – Independent Providers 2019

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
- Recognize your ongoing compliance responsibilities
- Know how to contact the Corporate Responsibility (CR) Department

Message from President and CEO

Regional 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
Regional Health

Corporate Responsibility

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

The department reports directly to the Compliance, Audit & Compensation Committee of the Regional 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.

Compliance Program

Regional 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. Compliance Officer that is accountable and responsible for the program, and compliance committee.
    - Nancy Klunder, Vice President of Corporate Responsibility
3. Effective training and education.
4. Effective lines of communication for reporting compliance concerns.
    - Compliance Hotline
5. Disciplinary action for non-compliance of standards or policies.
6. Routine monitoring and auditing to identify risks.
    - Examples of audits: physician contracts, billing, coding, patient record access, etc.
7. Respond promptly to non-compliance and undertake corrective action.
    - Take action to address non-compliance and reduce likelihood of recurrence

Policy: Corporate Compliance Program

Fraud, Waste and Abuse

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.

Fraud, Waste, and Abuse

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.

Fraud, Waste and Abuse

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.

Fraud, Waste and Abuse

- 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.

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!***

EHR Compliance

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 Regional 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.

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 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 Regional 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.

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.

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.

Consent

- 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).
  - **<u>Exception</u>- 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;
- Any reasonable suspicion of a crime committed against a resident of a long-term care environment.

EMTALA

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.
- EMTALA requires all hospitals with a dedicated Emergency Department to screen all patients who request treatment to determine if they have an emergency medical condition or if they are in active labor.
  - We must stabilize the emergency medical condition or assist with labor within the Hospital's capability before transferring to another facility.

EMTALA

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)

EMTALA

Transfer to another facility may only occur if:

- The patient's emergency medical condition has been stabilized;
- The patient requests a transfer after being advised of the hospital's obligations under EMTALA;
- The hospital is unable to stabilize the patient within our capability;
- The provider certifies the benefit of transfer outweighs the risk for transfer to a hospital with capabilities to treat the emergency medical condition;
- The transferring hospital has provided medical treatment to minimize the risk; and
- The receiving hospital has:
    a. Available space and qualified personnel to treat the patient; and
    b. Agreed to accept the transfer and provide the appropriate treatment.

The transferring provider is responsible for meeting these requirements.

EMTALA

- Providers are obligated to provide on-call services to meet the requirements of EMTALA, in accordance with hospital policies and Medical Staff Bylaws.
- EMTALA obligations end when:
  1. The patient's emergency medical condition is stabilized;
  2. The patient is admitted as an inpatient; or
  3. An appropriate transfer has been accomplished.

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; and
- The patient cannot readily validate the ID information on file.

All registration/intake areas of Regional 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: Regional Health Identity Theft Program

HIPAA

What is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA).

What does HIPAA do?

- Requires Regional 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 & disclosures.
- Request alternative forms of communications.
  - Mail to P.O. Box, not street address
- Obtain a copy of their record.
- Request and accounting of the 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

HIPAA - Permitted Uses & Disclosures

When can you access, use, or disclose 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 - Permitted Uses & Disclosures

HIPAA permits PHI to be disclosed to 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. If 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 that in the medical record.
3. When there is a crime on premises
   - The PHI sought by law enforcement is evidence of a possible crime on RH 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 & 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 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 – Authorized Uses & Disclosures

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 & 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

Identification Badges:

- Wear your badge at all times; do not leave unattended.
- Do not allow anyone else to use your badge for access to healing environments, signing on to computer systems, meal or coffee purchases, etc.

Physical Access Awareness:

- Escort visitors to appropriate areas.
- Watch for tailgating; individuals entering a secured area by walking in behind someone with appropriate access.

Policy: Identification Badges

HIPAA Security – Safeguards

Malicious Activity or Internet Security Attacks:

Phishing is a particularly dangerous form of email spam that seeks to trick users into revealing sensitive information, such as passwords.

- Remember "SPAM" to stay safe:

S – Sender	• If you know the sender/company and the email is unexpected or suspicious, contact them directly for verification. • Always use caution when opening email from unknown sources.
P – Pause	• Check for poor grammar, editing errors, requests for personal information, or promises that are too good to be true.
A – Alert	• If the email or attachment seems suspicious contact the IT Help Desk. • Don't open email attachments or click on any links.
M – Message	• Review the message; check for anything out of place. • Hover your mouse over any links to verify what you are clicking on.

HIPAA –Protecting PHI

Paper

- Immediately gather documents you sent to a printer. Use "Secure Print" to avoid documents sitting on the printer.
- Lock up documents containing PHI when unattended.
- 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 "Regional Health".

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

HIPAA –Protecting PHI

Computer Security

- Lock/log off your computer when you are away from your workstation.
- Ensure information on monitors is not visible to passersby.
- Never leave mobile devices (iPad, laptop, etc.) unattended.
- Create a strong password and **do not share** your username or password with anyone.
- Do not write your password down; store securely (e.g., 'J' drive).

Policy: Information Security – Acceptable Use of Information Technology Resources

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

HIPAA –Protecting PHI

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 texting/messaging apps to send PHI is not permitted as it is not secure or encrypted; only Regional Health approved and secure apps may be used, such as Haiku, Canto, and Rover.
  - Contact the IT Help Desk if you have questions about 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 Regional Health device
    - » Use a personal device only when logged into a secure, Regional 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 –Protecting PHI

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 – Breach

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.

HIPAA – Breach

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 Regional Health provider is to report privacy or security breaches involving PHI.

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

- **Action**: Ask the recipient to shred or return the information.
- **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 Forms/Provider Orders located on the left-hand side of the home page and search by "Suspected".
- **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

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

Regional 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

If you suspect violations regarding billing, HIPAA, EMTALA, safety, or any other topic covered in this training, ***please report immediately***.

- Reporting Options
  - Management/Physician Leadership/Administration
  - Corporate Responsibility department at (605) 755-9020
  - Compliance Hotline (can report anonymously)
    - 1-877-800-6907 or https://RegionalHealth.alertline.com
    - Electronically via the link on the 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

Corporate Responsibility Hub Page

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

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

Compliance & Ethics Training – Independent Providers

You have completed the Compliance & Ethics Training Module for Independent Providers. Please record your confirmation number for completion, 768183.