2019 REI Corporate Compliance Handbook

- **Memorial Medical Center, Inc.**
- **Hayward Area Memorial Hospital&Water's Edge**
- **REI Medical Clinics, Inc.**

Purpose Statement:
This booklet is to bring important compliance information to the attention of individuals providing a service to REI and keep it available so that it may be readily accessible to these individuals and affiliate personnel. Through this process we can continue to demonstrate that REI facilities are committed to conducting business honestly, legally, and ethically. This booklet does not replace specific policies your organization may have in place.

Table of Contents

COMPLIANCE PROGRAM

After reading this information individuals will be able to understand the makeup of the C*ompliance Program*, the *Code of Conduct*, and state the *compliance hotline number*.

The purpose of the *Compliance Program* is to demonstrate to the community at large and all employees that the healthcare facility is committed to conducting business honestly, legally, and ethically. The government is very focused in their efforts to combat healthcare fraud and continue to invest time and money in cracking down on both payers and providers of healthcare services. Therefore, it is with this program that we will educate staff about compliance, train staff to be compliant, provide staff with the tools and procedures to carry out compliance, and rely on staff to make our compliance program effective.

The Compliance Program is based on the Office of Inspector General's (OIG) Compliance Program Guidance for Hospitals and the Compliance Program Guidance for Nursing Facilities. Within these guidance programs there are specific elements that the OIG says should be implemented into the compliance program. They are:

1. Development and distribution of a written *Code of Conduct*.
2. Designation of a compliance officer and compliance committee.
3. Development and implementation of effective education and training programs.
4. Develop a reporting process to receive complaints, including a process such as a hotline to protect anonymity and protect against retaliation.
5. Develop a system to respond to compliance allegations and enforce appropriate disciplinary action against employees who have violated

compliance standards or laws.

6. Develop auditing or other evaluation techniques to monitor compliance and assist in the reduction of risk areas.
7. Develop a system for investigation and remediation of identified problems to include a policy addressing the non-employment or retention of sanctioned individuals.

Within our healthcare organization there are numerous policies and procedures, rules and regulations, and laws that affect our day to day duties that we perform in order to carry out our specific jobs. Employees will be educated and trained in these areas through new employee orientation, probation training, annual inservice training, and internal and external educational opportunities. Compliance education is an on-going process.

The *Code of Conduct* is one means of educating employees and "agents" (those authorized to act on behalf of our facility) of our compliance program. The code is made up of broad statements regarding compliance areas and provides a brief overview of certain behavioral and policy matters of the facility. The code is not intended to replace official policies and procedures or company manuals. Employees should look to official policies and procedures and company manuals for more detailed information regarding their concerns. It is your duty as an employee to report any instances of possible violation of these standards and it is important to understand that any violation, by action or inaction, is beyond the scope of employment and subject to disciplinary action. This is the most public of all our compliance statements and all employees and agents will receive a copy of the *Code of Conduct* and will be required to sign a statement that they have received and reviewed the *Code of Conduct*.

Involvement, communication and reporting are key to the effectiveness of our compliance program. The healthcare facility endorses and maintains an "open door" policy when it comes to employee reporting. Employees are encouraged to first go to their supervisors and follow the chain of command when reporting an allegation, incident or any concern. However, a compliance concern can be communicated to any staff member and then the staff member will communicate that concern to the appropriate personnel for follow-up. The facility also has in place a non-retaliation policy so employees can report concerns without having to worry about any type of retaliation. It is important for employees to understand that they should follow up on their concern until it is resolved no matter what the outcome may be. If for some reason the employee is not comfortable with this procedure the Compliance Officer can always be contacted. The Compliance Officer can be contacted at **(715) 685-5185** or at extension **5185.** The OIG also states that a facility should have an option, such as a hotline, for employees to use when reporting a compliance concern, which would protect their anonymity and protect against any retaliation. The facility does have in place a *Corporate Compliance Hotline*. The hotline number is **1-866-680-7960**. This is a toll free number and is available 24 hours a day, seven days a week.

Employee Reports to JCAHO (applies to Memorial Medical Center only). Employees are encouraged to identify any safety or quality of care issue and report it to the appropriate manager. If the staff member does not wish to report the concern to a manager or if the staff member feels the issue has not been resolved following such report, any staff member may report a safety or quality of care issue directly to the Joint Commission. MMC is committed to protecting employees against any retaliation for making such a report and will take no disciplinary action against any employee for reporting a safety or quality of care concern to the Joint Commission.

MMC employees are informed of their right to report safety and quality of care concerns directly to the Joint Commission as part of new employee orientation. MMC employees may contact the Joint Commission directly on their website or by phone. The Director of Compliance is another resource to employees who wish to make such a report.

REI employees, please keep your *Code of Conduct* in a place so that you can make reference to it if you should have a compliance concern. If you do not have a copy of the *Code of Conduct* you may obtain one from the compliance officer or it can be found in and copied from the organization website (Right Here). Also do not hesitate to bring any concern to your supervisor or the compliance officer if need be. Remember the hotline number (**1-866-680-7960**) as an option to reporting a compliance concern.

Centers for Medicare & Medicaid (CMS) Fraud, Waste, and Abuse Training

As part of their continuing efforts to raise awareness to, and to detect, prevent and correct fraud, waste and abuse, CMS is requiring that Sponsors of Medicare Advantage Organizations (MAOs) and Prescription Drug Plans (PDPs) annually train their direct employees and all entities they are partnering with to provide benefits in the Part C and Part D programs in the area of Fraud, Waste, and Abuse. It is further required that we track our organization's training by maintaining a log of individuals that have signed off after completion of the training, and to file an attestation form with health plans we are contracted with.

CMS determined the following topics should be included in the Fraud, Waste and Abuse training program.

Definitions-

Plan Sponsor: An entity that has a contract with CMS to offer one or more of the following Medicare Products: Medicare Advantage (MA) Plans, Medicare Advantage Prescription Drug Plans, Prescription Drug Plans (PDP) and 1876 Cost Plans.

Fraud: an intentional act of deception, misrepresentation or concealment in order to gain something of value. Examples may include: billing for services that were never rendered, billing for services at a higher rate than is actually justified and deliberately misrepresenting services, resulting in unnecessary cost to the Medicare program, improper payments to providers or overpayments.

Waste: over-utilization of services (not caused by criminally negligent actions) and the misuse of resources.

Abuse: excessive or improper use of services or actions that are inconsistent with acceptable business or medical practice. Refers to incidents that, although not fraudulent, may directly or indirectly cause financial loss. Examples may include: charging in excess for services or supplies, providing medically unnecessary services, and billing for items or services that should not be paid for by Medicare.

Compliance Program-

Regional Enterprise Inc. (REI) maintains a compliance program that is based on the Office of Inspector General's (OIG) 7 core elements put forth in their Compliance Program Guidance for Hospitals and Nursing Facilities. Policies and procedures are in place to ensure compliance with these elements. Please refer to the section, Compliance Program, of this booklet for more information.

Federal Fraud, Waste, and Abuse Laws-

There are many laws in place to help detect, prevent and

correct fraud, waste and abuse such as:
False Claims Act: Prohibits any person from knowingly presenting or causing a fraudulent claim for payment. Refer to the section, False Claims Act, of this booklet for more information.

Anti-Kickback Statute: Makes it a crime to knowingly and willfully offer, pay, solicit, or receive, directly or indirectly, anything of value to induce or reward referrals of items or services reimbursable by a Federal health care program.

Self-Referral Prohibition Statute (Stark Law): Prohibits physicians from referring Medicare patients to an entity with which the physician or a physician's immediate family member has a financial relationship, unless an exception applies.

There are many types of fraud, waste and abuse that can occur at different levels and in different entities, such as, Prescribers, Wholesalers, Beneficiaries, Pharmaceutical Manufacturers, Plan Sponsors, Pharmacy Benefits Managers, and Billing. Some examples that could be applicable to our facilities might include, identity theft, billing for services not provided, misrepresenting the service that was provided, billing for a higher level than the service actually delivered, and billing for non-covered services or prescriptions as covered items.

Additional information is available from ***Security Health Plan's Compliance Tool Kit*** which you can find on MMC's intranet Right Here, under Department, then click on Compliance or you can link directly to it HERE.

It is everyone's right and responsibility to report possible fraud, waste and abuse. There are different methods in place for individuals to report issues or concerns such as, reporting to a supervisor or department manager, reporting to the compliance officer, privacy officer, or security officer, utilizing

the compliance hotline (1-866-680-7960), utilizing Plan Sponsor's hotlines available on their websites, and 1-800-MEDICARE.
Refer to the Compliance Program section of this booklet, your Code of Conduct, specific policies, and the last page of this booklet for more information and important related individual contact information.

Remember: You may report anonymously and retaliation is prohibited when you report an issue or concern in good faith.

FALSE CLAIMS ACT

In 2005, Congress passed the *Deficit Reduction Act* (DRA) which mandates changes specific to the Medicaid program to combat fraud, waste, and abuse. The DRA provides an increase in the state's share of recovery in Medicaid fraud if the state has its own law similar to the federal ***False Claims Act*.** The DRA also imposes new compliance and education requirements on healthcare organizations based on certain criteria. These changes became effective January 1, 2007.

The following are some of the things you should know about false claims.

- A *false or fraudulent claim* is a request for payment for a medical service or item that is not reasonable or necessary for the diagnosis or treatment of the patient.
- The submission of a false or fraudulent claim for a medical service or item to a federal government healthcare program is prohibited by the federal *False Claims Act* and may also be prohibited by similar state laws.
- Employees who report the submission of false or fraudulent claims to appropriate governmental agencies are protected as "whistleblowers" and may

not be retaliated against on their jobs.

- Our policies and procedures cover detection of fraud, waste, and abuse. Questions concerning false claims to federal or state healthcare programs or any instance of fraud, waste, or abuse should be directed to our compliance officer. The phone number for the compliance officer is (715) 685-5185; internally you can call extension 5185.

What is a false claim? The basic rule in billing for services under federal healthcare programs is: no payments shall be made for services or items, which are not reasonable or necessary for the diagnosis and treatment of the patient. *A false or fraudulent claim, then, is a request for payment for a medical service or item that is not reasonable or necessary for the diagnosis or treatment of the patient*. Upcoding and unbundling of claims are examples of false or fraudulent claims.

Under the *False Claims Act* (FCA) misconduct that is related to the submission of claims to federal healthcare programs (*e.g., Medicare, TRICARE, Medicaid, etc.*) can be grounds for a civil suit, criminal prosecution, or administrative remedies. Some of the consequences for this kind of misconduct are as follows:

- A provider that is found civilly liable under the FCA must pay treble damages, or three times the amount of loss to the federal government, as well as civil fines of up to $11,000 for each false claim,
- Criminal sentences (e.g., jail time) can be imposed for certain kinds of fraud, and
- Administrative remedies such as nonpayment of the claim, civil monetary penalties, or a provider's exclusion from federal healthcare programs may also be imposed.

The FCA applies to any person or entity who knowingly presents a false or fraudulent claim to the government for approval or payment. To encourage reporting of false or fraudulent claims to the government or a law enforcement agency, the FCA protects employees who are "whistleblowers" from retaliation (e.g., loss of job, demotion, etc.). As an incentive for reporting fraud, individuals may, in limited circumstances, share in the money recovered by the government through successful prosecution of false claims. State laws against false claims may also impose similar penalties.

Our compliance program is based on policies and procedures for detecting and reporting fraud, waste, and abuse. Under these policies and procedures, as well as applicable federal and state laws, you are protected from retaliation for reporting false or fraudulent claims. Our policies and procedures apply to all of our employees, as well as to outside contractors. If you suspect any fraud, waste, or abuse, please contact the compliance officer.

CONFIDENTIALITY and the PRIVACY RULE

It is a patient's right to expect that his/her health information be treated with the utmost privacy and confidentiality. This trust allows patients to speak freely with their physician and other caregivers about their medical or mental health condition. As REI employees, it is our responsibility to respect this patient right and to strictly maintain the confidentiality of patient information.

A federal law called HIPAA *(the Health Insurance Portability*

and Accountability Act of 1996) makes the privacy of health information not only an ethical practice but also the law. A provision of HIPAA called the Privacy Rule sets forth federal laws which govern patient privacy and confidentiality.

Under the Privacy Rule, confidential patient information is called protected health information (PHI). Protected health information is defined as any information about a patient that relates to his/her past, present or future health or mental health condition.

- PHI is information that can identify a patient.
  - It includes such obvious information as name, birth date, social security number and address.
  - It also includes less obvious information such as e-mail address, license plate number and even physical characteristics such as scars and tattoos.
- Protected health information can be in electronic, written or verbal format.
- Protected health information is confidential information.

A patient's protected health information can only be used or shared

- by health care workers involved in the direct care of the patient such as physicians and nurses, or
- by employees who need the information to do their jobs such as billing staff, coders or utilization review staff.
- The amount of PHI accessed should always be the **minimum amount necessary to do your job effectively**.
  - You should always ask yourself, "Do I need this information to do my job? What is the minimum amount of information I need to do my job?"

Although all PHI is confidential, PHI related to the treatment of alcohol, drugs or mental health has an even greater level of confidentiality. This is due to the sensitive nature of information that must be disclosed during the treatment

process. State and federal law strictly protect this information.

Protected health information should not be shared with co-workers who are not involved in the care of the patient. A patient should never be discussed outside of the work setting. Hospital staff should never discuss protected health information in public areas such as the cafeteria or elevators. Staff must be mindful of discussing protected health information in an area where a visitor or a co-worker not involved in the patient's care might over hear.

PHI on computers must be also be safeguarded.

- It is important that the public can not view computer terminals that display PHI.
- When leaving a computer, never allow protected health information to remain on the screen
- It is always a good practice to minimize your screen or if possible, log off or use control/alt/delete to lock your screen.

Designated individuals (physicians, nurses) may share PHI with a patient's immediate family if the patient has given his/her authorization to do so.

- Immediate family is the spouse of an adult patient, adult children, parents of a child or a patient's legal guardian.
- We honor a patient's request that information not be shared with others, even with family members.

In most instances, protected health information can only be released with the written authorization of the patient. However, an authorization is not required to release information for treatment, payment or health care operations. (Health care operations include such business practices such as quality assurance activities, utilization review and audits.)

A more specific authorization signed by the patient is required to use or disclose protected health information for any other purpose.

It is a patient's right to choose whether or not he/she wants to be included in the hospital's Facility Directory. This directory is the list of hospital inpatients that want to receive visits or telephone calls from relatives and friends. The Facility Directory includes the following information:

- patient's name
- location in the hospital
- condition in general terms (see Inquiries from the media)
- religious affiliation (for clergy only)

If a patient wishes to be in the directory, the patient's location in the hospital can be given to callers or visitors if they ask for the patient by name. If a patient "opts out" of being in the facility directory, hospital staff cannot give out any information about the patient, even the fact that the patient is in the hospital. If a patient wishes to be in the Facility Directory and gives a religious affiliation, a member of the clergy may obtain information of patients for his/her religious denomination so a pastoral visit can be made.

PHI can only be faxed to another facility in an emergency or when it is absolutely necessary to assure continuous patient care.

- Non-urgent patient information should be sent via mail.
- Discretion must be used to send only the information requested.
- It is important to verify that someone from the receiving facility will be available to receive the faxed information when it is sent.
- Extreme caution must be used in the event that information **involving drug or alcohol treatment or**

information involving sexually transmitted disease must be faxed.

- The faxing of this information is strongly discouraged by REI policy.

All PHI should be disposed of in the Shred It bins. Even post it notes or a scrap of paper can contain PHI and should be disposed of properly.

Inquiries from the media or a government agency must be referred to Administration, Public Relations or the Nursing Supervisor.

Any staff member who uses or discloses PHI improperly has committed a **breach of confidentiality.** This is a serious offense at our hospital that can result in discipline up to and including immediate dismissal.

Under the Privacy Rule, a breach of confidentiality can also result in a civil or criminal suit to include fines and/or imprisonment. However, the most severe penalties involve "malicious intent" or "willful neglect"; malicious intent is, knowingly using or disclosing protected health information with intent to harm the patient or hurt the institution. Willful neglect is the conscious, intentional failure or reckless indifference to the obligation to comply with HIPAA.

The HITECH Omnibus Final Rule includes modifications to the HIPAA Privacy and Security Rules and authorizes increased payments for violations under these rules. This law went into effect on March 26, 2013. The key changes of the HITECH Final Rule include:

- The notification of an individual(s) whose PHI has been breached.
- An individual's right to access a copy of their PHI maintained electronically in electronic format.

• The right of the individual to request restrictions of PHI to a health plan or insurer when the individual has paid for items or services out-of-pocket, in full.

Confidentiality is everyone's business. It is every patient's right to know that his/her PHI is kept safe and secure from unlawful access, tampering or unauthorized release. It is our obligation to assure that a patient's right to privacy is maintained.

Other References:

- Confidentiality: Who Needs to Know
- Keep it to Yourself: Protecting Patient Confidentiality
- HIPAA Privacy Compliance
- Confidentiality, Privacy and HIPAA
- The HITECH Omnibus Final Rule

HIPAA Security Rule

Another piece of HIPAA (*Health Insurance Portability and Accountability Act of 1996*) is the Security Rule. Like the Privacy Rule it is all about taking appropriate measures to ensure the security of protected health information (PHI), particularly in electronic form. Whereas, the Privacy Rule states that covered entities must protect PHI in any form, (verbal, written, or electronic), the ***Security Rule*** focuses on the electronic form.

Similar to the Privacy Rule requirements, the facility has put in place policies and procedures to address the Security Rule requirements. These policies and procedures can be found in the Hospital Portal policy software

within the facility computer system.

The Security Rule is divided into three parts. They cover policies, procedures, processes and systems needed to protect electronic protected health information (ePHI), from the time it is created to its disposal and everything in between. The three parts are:

- *Administrative safeguards*-includes on-going risk analyses and creating policies and procedures to safeguard all ePHI.
- *Physical safeguards*-protection of physical things such as computer systems and other equipment as well as the facility where ePHI is stored. (Name badges, passwords, user IDs, workstation controls, auto log-off, etc.)
- *Technical safeguards*-all the technology that makes physical safeguards possible. (Access controls, virus checking, transmission controls, monitoring systems, etc.)

Some important points to remember are:

- E-mail: This is the most common way to infect a system. Do not open personal e-mail or suspicious e-mails where you don't know the sender or are unfamiliar with the subject or has suspicious attachments. Do not send
  e-mails, outside of the facility, that contain ePHI.
- Software: Don't load any software without checking with the IS department first. Don't open any suspicious pop-ups on the internet.
- Workstations: Keep sensitive material confidential and out of the public's eye especially if your workstation is accessible to the public. When you are away from your workstation, lock your workstation so no one can access it or log-off your workstation. Be aware of your surroundings, what is happening in the area and who is in the area.

Ask to assist people if they seem out of place.

- **Don't share your password with anyone!**

Breach Notification

The federal economic stimulus bill, also known as the American Recovery and Reinvestment Act (ARRA) of 2009, was signed by President Obama on February 17, 2009. To increase the use of the electronic health record, this law provides financial incentives to hospitals, physicians, and others to implement and use an electronic health record.

However, as the use of the electronic health record (EHR) increases, so do the number of privacy breaches, security breaches, and the incidence of identity theft. To counteract these increased risks, the HITECH Act (which is part of ARRA) strengthens privacy and security protections for health information and "plugs the holes" in the basic HIPAA regulations.

The Privacy Rule states that **a breach of information is acquiring, accessing, using, or disclosing protected health information** that is not permitted under the Privacy Rule and which compromises the privacy and security or integrity of the PHI

Examples of breaches are:

- Employee accesses the electronic health records of anyone out of curiosity/without a need to know or a business related purpose.
- Employee leaves reports containing PHI in a public area or on a photocopy machine.

- Employee misdirects an e-mail or fax containing patient information to the wrong person or organization.
- Employee sends records, bills, or reports to the wrong person or organization.
- Employee posts a patient's information on any Social Networking sites.
- EMT takes a cell phone picture of a patient in the ER after a car accident and sends the photo to friends.
- Employee finds his laptop, PDA, or flash drive which contains PHI to be lost or stolen.

The new HITECH Law **requires patients to be notified promptly** when there is a breach of their protected health information. The Privacy Rule did not require this. However, not all privacy and security breaches will result in breach notification. Breach notification occurs only when the breach poses a significant risk of financial, reputational, or other harm to the individual(s).

When a breach is discovered, the hospital must take the following steps:

- Initiate a breach investigation.
- Perform and document a risk assessment.
- If the breach results in harm to the individual(s), notify the individual(s) by mail within 60 days of the breach.
- Maintain a breach notification log and submit the log to the Secretary of Health and Human Services (HHS) at the end of the year.
- If the breach involves over 500 patients, also notify the media and the Secretary of HHS.

The Secretary of Health and Human Services may impose fines for breaches, based on the extent of the breach and the harm it caused. These fines are higher than those originally

imposed under the Privacy Law. Fines can be imposed against the individual and/or the facility.

Under HIPAA, the Privacy Rule mandates a sanction policy which describes the appropriate sanctions against members of its workforce who fail to comply with privacy policies and procedures. A breach, particularly if there is significant harm to the patient, will be subject to disciplinary action which may result in immediate termination.

To avoid committing a breach, you should:

- Follow all confidentiality and HIPAA policies.
- **Only access patient information needed to do your job – do not snoop around or gossip about a patient.**
- Use extra care when sending faxes to assure the fax does not go to the wrong place.
- Do not leave PHI unattended or leave it in a public place or on a photocopy machine.
- Do not remove patient information from the hospital without permission and without taking extra precaution to prevent it from being lost or stolen.

Finally, if you feel a breach has occurred, as referenced by MMC's Breech Notification policy, please report it **immediately** to your immediate supervisor, the facility's Privacy Officer, the Compliance Officer (X5185), or Administration.

EQUAL OPPORTUNITY

As part of our customer service standards, it is an expectation for all employees to demonstrate an awareness of the value of diversity in our communities and our workforce.

To help us do this, REI has established an ***Equal Opportunity and Affirmative Action Plan.*** The goal of a Civil Rights Compliance Plan is to have the number of women, minorities, and disabled people in our patient population and our workforce reflect the diversity of the communities that we serve. The Plan includes procedures for assessing the number of women, minorities, and disabled people, which comprise our patients, our workforce, and our communities. This assessment has demonstrated that these groups are well represented in our patient population. Women are very well represented in our workforce, minorities and disabled people are fairly well represented. The Affirmative Action Plan has established goals to help our workforce become more representative of the diversity that we find in our communities.

Equal Opportunity is not just a customer service goal of REI; it is a requirement to comply with state and federal laws and to meet the requirements of service contracts which REI maintains. Title VI of the Civil Rights Act of 1964 states that "*no person shall on the grounds of race, color, or national origin be denied the benefits of, or be subjected to discrimination under any program or activity receiving federal financial assistance*." Over time

other federal laws, Wisconsin state laws, and court decisions have extended this protection against discrimination to additional groups of people such as women and people over the age of 40. More recently, protections offered to people of different national origins have heightened concern about removing eligibility barriers for people who have little or no understanding of English. These groups are known as *Limited English Proficiency Groups* [LEPs].

New requirements now exist to ensure meaningful access to healthcare services for LEP persons. Although the number of non-English speaking people in our service area is minimal, we do encounter this situation from time to time. If you should encounter a patient or family member who does not understand English well, refer to the Patients with Language Barriers Policy and contact an RN Supervisor. The RN Supervisor has access to an interpreter service for any patient who has limitations speaking and/or understanding English or who is hearing impaired. See Limited English Proficiency Policy and Hearing Impaired Policy. REI is obligated to provide free oral interpretation for any patient who has limitations in speaking and understanding English or is hearing impaired.

REI maintains a written complaint procedure regarding equal opportunity and civil rights compliance. Notices regarding its availability are posted for both the public and REI employees. The Affirmative Action Plan and Civil Rights Compliance Plan are available for review. The Compliance Officer of Regional Enterprises Incorporated, has been appointed as REI's Equal Opportunity Officer and as the Limited English Proficiency Officer. REI is also committed to providing ongoing training for employees to increase understanding and awareness of different cultures and civil rights issues. Our goal is to remove as many obstacles of this kind as possible for community members who may need our services or who may want to work at REI. For further information, review the

Equal Opportunity and Affirmative Action Policy, the Limited English Proficiency Policy, the Hearing Impaired and the Affirmative Action Policy and Plan found in RIGHT HERE.

Questions or concerns?

MMC Administration @ 715-685-5510
HAMH/WE Administration @ (715) 934-4247

Anna Skar, HAMH & WE, Human Resources Director @ 715-934-4321

Lisa Ekman, Health Information Director
MMC Privacy Officer @ 715-685-5535

Diane Lulich, MMC Human Resources Director @ 715-685-5521

REI Compliance Officer @ 715-685-5185

Sharron Probyn, HAMH & WE Privacy Officer @ 715-934-4258

Todd Reynolds, REI HIPAA Security Officer & Director of Information Systems @ 715-685-5588

Compliance Hotline: 866-680-7960

Signature Page

I have received and read the 2019 REI Corporate Compliance Handbook. I understand the contents of the information contained in this booklet and understand that if I have questions that I may contact REI's Compliance Officer or Administration for any questions I might have:

REI Compliance Officer
Phone Number: (715) 685-5185

Printed Name

Signature

Title

Date

***REI Corporate Compliance* 2019**

Handbook

REI Compliance Officer
Phone Number: (715) 685-5185

Note! This book is regarded as resource material and is not intended to replace specific policies or annual Inservice. This book is to be retained for your reference.
Thank You.