SUPLIER, VENDOR, CONTRACTOR COMPLIANCE EDUCATION

Corewell Health

Partner | Educate | Advise

Priority Health

Topics Covered in this Training:

- Code of Excellence
- Compliance Program
- Fraud, Waste and Abuse
- Stark Law / Anti-Kickback Statute
- False Claims
- Whistleblower Protection / Non-Retaliation
- Reporting - Integrity Helpline
- HIPAA Privacy Rule
- Protected Health Information
- Auditing and Monitoring
- HIPAA Security Rule
- Safeguarding Sensitive Data
- Artificial Intelligence
- Protecting Credit Information
- Social Media

Corewell Health Code of Excellence

This Code of Excellence (Code) applies system-wide to all employed and non-employed team members (collectively referred to as team members) including providers, contractors, consultants, agents, students, volunteers and suppliers.

1. **We do the right thing.** We do the right thing no matter if anyone notices or is watching. This includes conducting ourselves in accordance with our values, adhering to all professional standards for responsible and ethical business practices and complying with all laws and regulations governing our business. We acknowledge that it isn't always easy to do the right thing. If we are unsure of the right thing to do, we ask for help.
2. **We make sure everyone has a voice.** We raise concerns and we evaluate them through a fair and just culture. We do not allow retaliation against anyone seeking help or raising a concern in good faith. When human error happens, we support our team members through a non-punitive response.
3. **We treat everyone with compassion, dignity and respect.** We will serve everyone in our communities, without regard to race, color, sex, national origin, handicap/disability, age, HIV status, marital status, sexual orientation, gender identity, gender expression, religious beliefs, sources of payment for care or other protected status or category. We work to create environments free of harassment, violence and intolerance.
4. **We value diversity, equity and inclusion.** We embrace a diverse and inclusive organizational culture that fosters respect for all. At the same time, we acknowledge that inequities persist in our communities. We pledge to listen deeply and engage authentically with those impacted by systemic racism, so we can partner with others toward the goal of achieving health equity.
5. **We maintain a healthy workplace.** We promote a positive work environment for everyone. We act in safe and healthy ways and do our jobs with clear minds.
6. **We are good stewards of our resources.** These resources include our people, facilities, funding, information, technology, equipment, and supplies. We use them responsibly, and ensure that others do, too. We share them or allow others access to them only for legitimate business purposes and with proper authorization.
7. **We code and bill our services appropriately.** We strive to ensure and maintain complete and accurate documentation of medical services provided. We expect accurate coding from our provider partners. We report and return any overpayment once identified from a government health care program, commercial payer, or patient.
8. **We are transparent with quality and pricing.** We give clear and accurate information as it relates to charges for the items and services we provide. We proactively share information about the quality of our care, the outcomes of our services, and the experiences of our patients and health plan members. We attempt to answer questions and resolve disputes related to our services to the patient's, health plan member's and payer's satisfaction.
9. **We protect the confidentiality and privacy of our patients and health plan members.** We collect information about a patient's and health plan member's medical condition, history, medication and family illnesses to provide the best possible care and health plan services. We protect individuals' health information while allowing the flow of information needed to provide and promote high quality health care.
10. **We are honest, accurate and fair in our business relationships.** We provide true and accurate information to the public, regulatory agencies, news media, and others who have an interest in our activities. We engage in social media in a way that is truthful and respectful of others. We follow our policies and principles of good business ethics pertaining to the exchange of gifts and business courtesies with suppliers. We address potential conflicts of interest before they arise, and when they do arise, we manage them through disclosure and removing the individual(s) with the conflict from decision-making related to the interest or matter.

How Can I Report a Concern?

You can report a concern in several ways. Our help lines are available 24 hours a day, seven days a week. An outside company receives calls and online submissions. The Compliance Department receives the report and reviews for follow-up or investigation. All contacts are confidential, to the limit allowed by law. If you prefer, you can make an anonymous report. Providing as much information as possible will help us review the validity of the report and investigate any potential misconduct.

Corewell Health
Integrity Help Line
877.319.0266
Integrity Help Line

Priority Health
Integrity Help Line
800.560.7013
*For providers, vendors, agents and members

You can always contact the following team members:

Corewell Health
Leah A. Voigt, JD, MPH
Chief Compliance Officer
Leah.Voigt@corewellhealth.org
616.486.2430

Priority Health
Cindy Rollenhagen
Compliance & Privacy Officer
Cindy.Rollenhagen@priorityhealth.com
616.464.8424

Corewell Health East
Michele McDonald
Compliance & Privacy Officer
Michele.McDonald@corewellhealth.org
947.522.2653

Corewell Health South
Chris Kuhlmann
Compliance & Privacy Officer
Christopher.Kuhlmann@corewellhealth.org
269.985.4600

Corewell Health West
Carrie Miedema
Compliance & Privacy Officer
Carrie.Miedema@corewellhealth.org
616.267.7518

Corewell Health Code of Excellence Acknowledgment

I understand and agree that:

- It is my responsibility to review, be familiar with, and comply with the Code of Excellence ("Code") and all related Corewell Health policies and procedures.
- Corewell Health and Priority Health provide an Integrity Help Line (877) 319-0266, managed by an outside, independent vendor for reporting (anonymously, if desired) any potential violation of the Code, Corewell Health policies or procedures, or any applicable laws, regulations or professional standards of conduct.
- I will not retaliate against another person for raising a concern or reporting a suspected violation of the Code, Corewell Health policies or procedures, applicable laws, regulations or professional standards of conduct.
- It is my responsibility to prevent, detect and report concerns and suspected violations of the Code or possible fraud, waste, and abuse, to a member of leadership, human resources, compliance, or the Integrity Help Line.
- I will inform my leader of potential conflicts of interest that I may encounter so that they may be properly addressed.
- If I violate the Code or other policies or procedures applicable to me as a Corewell Health team member, I may be subject to performance correction up to and including termination of employment or other relationship with Corewell Health and any of its affiliates, including Priority Health.

I certify that I am not currently excluded from participation in Medicare, Medicaid or any other federal or state health care program. I understand and agree that it is my responsibility to immediately disclose to the Corewell Health Compliance Department any current or future federal or state program exclusion or another event that makes me ineligible to perform work related directly to federal or state health care programs.

Electronic Signature: _____

Date: _____

Compliance Program

All related policies and procedures are available online through PolicyTech

Corewell Health™

Partner | Educate | Advise

Priority Health™

Compliance Program

Our Compliance Program consists if internal policies and procedures designed to ensure we're in compliance with required rules, regulations and laws to uphold our reputation as a top Health care provider.

Our Compliance Program:

- Demonstrates our commitment to following the required rules, laws and regulations
- Supports our Mission, Vision and Values
- Promotes ethical conduct throughout the organization
- Requires our policies and procedures to detect, prevent and correct potential issues

Elements of an Effective Compliance Plan

Our **Compliance Plan** is in accordance with the "Organizational Sentencing Guidelines" established by the Office of Inspector General (OIG) and contains the required **Seven Elements of an Effective Compliance Program**.

1. Implementing Standards of Conduct, Policies and Procedures
2. Establishing Compliance Oversight
3. Conducting Effective Training and Education
4. Developing Effective Lines of Communication
5. Conducting Internal Monitoring and Auditing
6. Enforcing Standards Through Disciplinary Guidelines
7. Investigating and Remediating Issues

Policies and Procedures are integral to day-to-day operations and essential tools help detect, prevent and correct potential compliance issues.

Our Code of Excellence sets clear expectations for team members.

Elements of an Effective Compliance Plan

Our **Compliance Plan** is in accordance with the "Organizational Sentencing Guidelines" established by the Office of Inspector General (OIG) and contains the required **Seven Elements of an Effective Compliance Program**.

1. Implementing Standards of Conduct, Policies and Procedures
2. Establishing Compliance Oversight
3. Conducting Effective Training and Education
4. Developing Effective Lines of Communication
5. Conducting Internal Monitoring and Auditing
6. Enforcing Standards Through Disciplinary Guidelines
7. Investigating and Remediating Issues

The responsibility for implementing, monitoring and overseeing the compliance program occurs at multiple levels: we have compliance officers, compliance committees and our board of directors through their compliance committees.

Elements of an Effective Compliance Plan

Our **Compliance Plan** is in accordance with the "Organizational Sentencing Guidelines" established by the Office of Inspector General (OIG) and contains the required **Seven Elements of an Effective Compliance Program**.

1. Implementing Standards of Conduct, Policies and Procedures
2. Establishing Compliance Oversight
3. Conducting Effective Training and Education
4. Developing Effective Lines of Communication
5. Conducting Internal Monitoring and Auditing
6. Enforcing Standards Through Disciplinary Guidelines
7. Investigating and Remediating Issues

We empower team members to do the right thing by providing education and training to ensure knowledge of federal, state and local regulations, accreditation standards, contractual obligations, along with internal policies and procedures.

Elements of an Effective Compliance Plan

Our **Compliance Plan** is in accordance with the "Organizational Sentencing Guidelines" established by the Office of Inspector General (OIG) and contains the required **Seven Elements of an Effective Compliance Program**.

1. Implementing Standards of Conduct, Policies and Procedures
2. Establishing Compliance Oversight
3. Conducting Effective Training and Education
4. Developing Effective Lines of Communication
5. Conducting Internal Monitoring and Auditing
6. Enforcing Standards Through Disciplinary Guidelines
7. Investigating and Remediating Issues

Compliance leadership and team members are here as a resource and partner for you. We provide third party reporting through our Integrity Help Line for all team members 24/7 with an anonymous reporting option.

Elements of an Effective Compliance Plan

Our **Compliance Plan** is in accordance with the "Organizational Sentencing Guidelines" established by the Office of Inspector General (OIG) and contains the required **Seven Elements of an Effective Compliance Program**.

1. Implementing Standards of Conduct, Policies and Procedures
2. Establishing Compliance Oversight
3. Conducting Effective Training and Education
4. Developing Effective Lines of Communication
5. Conducting Internal Monitoring and Auditing
6. Enforcing Standards Through Disciplinary Guidelines
7. Investigating and Remediating Issues

Performing planned audits, onsite visits, interviews and routine monitoring helps identify emerging risks as well as resolves issues in identified areas.

Elements of an Effective Compliance Plan

Our **Compliance Plan** is in accordance with the "Organizational Sentencing Guidelines" established by the Office of Inspector General (OIG) and contains the required **Seven Elements of an Effective Compliance Program**.

1. Implementing Standards of Conduct, Policies and Procedures
2. Establishing Compliance Oversight
3. Conducting Effective Training and Education
4. Developing Effective Lines of Communication
5. Conducting Internal Monitoring and Auditing
6. Enforcing Standards Through Disciplinary Guidelines
7. Investigating and Remediating Issues

The compliance department in conjunction with human resources establishes standardized guidelines for a fair and consistent approach to managing performance and conduct issues.

Elements of an Effective Compliance Plan

Our **Compliance Plan** is in accordance with the "Organizational Sentencing Guidelines" established by the Office of Inspector General (OIG) and contains the required **Seven Elements of an Effective Compliance Program**.

1. Implementing Standards of Conduct, Policies and Procedures
2. Establishing Compliance Oversight
3. Conducting Effective Training and Education
4. Developing Effective Lines of Communication
5. Conducting Internal Monitoring and Auditing
6. Enforcing Standards Through Disciplinary Guidelines
7. Investigating and Remediating Issues

All reports of concerns or issues are reviewed and investigated by the compliance department and compliance department partners who educate throughout the investigation process to ensure each report is resolved.

Fraud, Waste and Abuse (FWA)

Each of us plays a direct role in detecting, preventing and mitigating **fraud**, **waste** and **abuse**.

FRAUD: When someone intentionally deceives, makes a false statement or claim, or states that information they provide is true and correct, and it is not, it is considered FRAUD.

Situations that may be considered Fraud:

- billing for supplies or services not provided or performed
- intentional upcoding – altering a medical claim to receive higher payment
- intentional unbundling – billing separately for procedures that are all part of the same procedure
- knowingly adding an ineligible member or dependent

WASTE: Overuse of a service or other practice that results in unnecessary cost is considered WASTE. Waste is generally not considered to be caused by criminally negligent action but rather by the misuse of resources.

Situations that may be considered Waste:

- prescribing more medication than necessary for a specific condition
- wasting time by misplacing supplies
- ordering too many supplies

ABUSE: Abuse generally occurs when there is no intent to deceive.

Situations that may be considered Abuse:

- ordering excessive testing or performing more services than required
- using the emergency department as the family doctor
- using transportation services for non-related medical services

Laws Governing Fraud, Waste and Abuse

- There are many laws that govern health care fraud, waste and abuse:

- Stark Law (Physician Self-Referral Law)
- Anti-kickback Statute
- Deficit Reduction Act
- False Claims Act

Physician Self-Referral Law aka the Stark Law

What does this mean?
It means this law prohibits a **physician** from ordering any **Designated Health Service (DHS)** that is reimbursable by Medicare/Medicaid from any entity with which the physician or an **immediate family member** has a **financial relationship**.

The concern surrounding the Stark Law is that a physician may be more likely to order tests, or other services, if they stand to gain financially.

Anti-Kickback Statute (AKS)

Another important health care related law is the Anti-Kickback Statute (AKS). The **AKS** prohibits health care providers/suppliers from offering, paying, soliciting or receiving **anything of value** to induce or reward referrals or generate federal health care program business.

What does this mean?
It means that **ANYONE** who "knowingly and willfully" offers, pays, solicits or receives any compensation, is in violation of the Anti-Kickback Statute.

For example…

- Referring patients to friends and family members for services or treatment in return for a fee, bonus or kickback
- Accepting a "kickback" (some examples include coupons, gift cards, theater tickets) from a drug company when you switch a patient's prescription to their drugs
- Accepting material gifts or perks from vendors in exchange for selecting the vendor's products or services
- As a provider, receiving a fee for each patient who enrolls or remains enrolled in a plan

False Claims Act

The Federal False Claims Act (FCA) was passed as a result of fraudulent claims being submitted to the government: it applies to **anyone** submitting a claim for **any** item or service to **any** federal program.

Michigan Medicaid False Claims Act (MMFCA) is designed to prevent fraud, kickbacks and conspiracies in the Michigan Medicaid program. MMFCA allows a person (whistleblower) to file a civil lawsuit to recover losses to the state of Michigan. This law also contains important protections for whistleblowers who file claims in good faith.

The government defines a **CLAIM** as:

"a demand for payment or property made directly to the federal government or to a contractor or other recipient on behalf of the government."

A claim *does not need to be fraudulent* to be subject to FCA liability, it need only be false or wrong; meaning that it seeks something to which the submitter is not entitled.

Should we receive funds under a federal program which we are not entitled, we must report and return within 60 days of identification.

Penalties for Violating FWA Laws and Regulations

Civil Monetary Penalties Law (CMPL) or The Office of Inspector General (OIG) may impose civil penalties based on the type of violation. Listed below are the potential penalties for violating any of the Fraud, Waste and Abuse related laws or regulations (consequence will vary based on the violation).

Civil money penalties	Criminal conviction/fines	Civil prosecution
Imprisonment	Loss of provider license	Exclusion from federal health care programs
	Debarment from government contracts	

Whistleblower Protection Act / Non-Retaliation

A whistleblower is a person who reports **in good faith** information or activity that is illegal, unethical, or fraudulent against the federal government.

The following activities are protected activities under the Whistleblower Protection Act:

Reporting potential issues or concerns	**Investigating issues**	**Conducting self-evaluations**	**Audits**	**Corrective actions**

Ensuring Non-Retaliation

Once a whistleblower reports the potential fraud, they should not be subject to any form of **retaliation**, retribution or be discouraged or intimidated by another individual. For more information, review the **Non-Retaliation Policy**.

Because **retaliation** can be subtle, it may not always be easy to identify.

Some examples include demotion, denying overtime or time off, intimidation or harassment, making threats, withholding of special projects or work opportunities, exclusion from team meetings, reducing hours or schedule changes.

Integrity Help Line

It's important to **USE YOUR VOICE** to report a concern!

Reporting a concern helps us identify gaps in a process or where improvements are needed. It also helps us identify areas of risk.

WHAT should I report?

You should report any activity you question or believe violates a law, regulation, policy, professional or patient care standard, or the Code of Excellence, and any workplace safety or environmental concerns.

It's the responsibility of every team member to bring attention to and report any potential misconduct, unethical practice or safety issues.

For additional questions, see the **Integrity Help Line FAQs**

Integrity Help Line

It's important to **SPEAK UP** when you see something!

Reporting a concern helps us identify gaps in a process or where improvements are needed. It also helps us identify areas of risk.

HOW should I report?

Report concerns to your **leader**, the **compliance department** or via the **Integrity Help Line**.

The Integrity Help Line is managed by an independent vendor and is available 24/7.

We need to protect our patients and health plan members by reporting concerns.

Corewell Health
Integrity Help Line
877.319.0266
(reporting can be anonymous)

Here's How to Find Us

Contact us at:

Compliance Department

616-486-2430

compliancedepartment@corewellhealth.org

Privacy Team

616-486-4113

privacy@corewellhealth.org

Privacy Best Practices

All related policies and procedures are available online through PolicyTech

Corewell Health™

Partner | Educate | Advise

Priority Health™

What is HIPAA?

Ensuring patients' and health plan members' personal and health information is safe and private is a key part of developing trust with our patients and health plan members in order for Corewell Health to provide quality care.

The **Health Insurance Portability and Accountability Act** of 1996 (HIPAA) was created to protect the privacy of an individuals' health information while at the same time permitting needed information to be disclosed for patient care and other purposes. Legislation was developed for the **Privacy Law and** the **Security Law**, the two main components of HIPAA.

HIPAA Privacy Rule

The **HIPAA Privacy Rule** establishes national standards to protect individuals' medical records and other Protected Health Information (PHI) and applies to **covered entities***. Protected data also includes Personally Identifiable Information (PII)

The privacy rule:

Enforces safeguards to protect the privacy of PII, PHI and controls use and disclosures of that sensitive data

Requires ALL verbal, written and electronic information to be protected

Allows an individual rights over their protected health information, including:

- right to inspect and obtain a copy of their protected health information
- right to amend
- right to an accounting of disclosures - right to request restrictions
- right to request confidential communications
- right to a paper copy of Corewell Health's Notice of Privacy Practices

*Covered entities are defined in the HIPAA rules as (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with transactions for which Health and Human Services (HHS) has adopted standards.

Protected Health Information (PHI)

PHI is any information **created, received** or **stored** by a **covered entity*** (such as Corewell Health and Priority Health), including demographic data, that relates to:

The individual's past, present, or future physical or mental health condition;

The provision of health care to the individual; or

The past, present, or future payment for the provision of health care to the individual;

AND

That identifies the individual **or for which there is a reasonable basis to believe that information can be used to identify the individual**.

HIPAA Privacy Rule protects PHI for 50 years following the date of death of a patient - team and family members still need required authorization.

*Covered entities are defined in the HIPAA rules as (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with transactions for which Health and Human Services (HHS) has adopted standards.

What are the 18 Patient Identifiers?

1. Names
2. All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death
4. Phone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code

It is recommended to use **at least 2 patient identifiers** to identify patients

Treatment, Payment, Operations (TPO)

Under HIPAA, patient authorization is not needed to use PHI for TPO purposes:

Treatment

The provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a patient and referral of a patient by one provider to another

Payment

Billing, coding, claims management, insurance payments, collection and related health care data processing

Health Care Operations

Quality and process improvement activities, re-certification, system auditing functions and underwriting and other activities related to the contracting of health insurance or benefits

Additional written authorization must be obtained from a patient for all uses and disclosures of PHI other than for Treatment, Payment or Health Care Operations (TPO). **The following items are NOT covered under TPO:**

- Marketing
- Research
- Uses not otherwise permitted
- Release of Information

Minimum Necessary

We must make every reasonable effort to limit use, access and/or disclosure of PHI to the minimum information necessary to accomplish a task required for your job.

Patient's entire medical history

What you actually need

- ✓ Follow minimum necessary requirements
- ✓ Pay attention to avoid mistakes
- ✓ Report and mitigate all mistakes with PHI
- ✓ To access your own medical information, you should view your medical records in MyChart or contact Health Information Management
- ✓ Unauthorized accessing of PHI or medical plan information could result in disciplinary action, up to and including separation from employment

Applicable Policies:

Minimum Necessary Requirements for Uses and Disclosures of Protected Health Information Policy

Using and Disclosing Protected Health Information

Pause before Sharing

Even though it might be accidental, misdirected PHI can be very harmful to our patients and health plan members. It is everyone's responsibility to double-check PHI for accuracy and ensure only minimum necessary is shared to protect our patients and health plan members.

Take the time to check it twice!

- Be aware of who is listening before discussing PHI
- Check the accuracy and spelling of any recipient email addresses
- Review the entire email chain and delete any unnecessary PHI
- Confirm a minimum of 3 patient identifiers to ensure that sensitive information provided or sent is for the correct patient or health plan member

Sending a fax?
Call ahead to verify the fax number and alert personnel to retrieve the fax immediately.

Reporting exposed PHI?
Notify your leader and the Privacy team privacy@corewellhealth.org if you have identified misdirected PHI.

Auditing and Monitoring

The privacy team utilizes technology to identify suspicious access to PII or PHI in applications such as EPIC. Access reviewed includes but is not limited to:

Accessing PII or PHI of a family member, friend, team member or oneself

Accessing PHI that is not customary for the job role

Accessing PHI outside of departmental/TPO purposes

You may mistakenly access the wrong record.

Back out of the record as quickly as possible and **report** it to your immediate supervisor and the privacy team.

The privacy team investigates cases flagged by the tool as suspicious. ALL team members are accountable for their actions and PHI access under their login. Inappropriate access to PHI, regardless of intent, can result in corrective action, **up to and including separation from employment.**

HIPAA Security Rule

The **HIPAA Security Rule** requires we maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI.

Specifically, we must:

- Ensure the confidentiality, integrity, and availability of all e-PHI we create, receive, maintain or transmit;
- Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- Protect against reasonably anticipated, impermissible uses or disclosures; and
- Ensure compliance by the workforce.

The **Acceptable Use Policy** governs the use of Corewell Health computing systems, which team members are required to follow to ensure that day-to-day operations and interactions with digital systems are secure.

Keep User IDs and Passwords Private, Safe and Secure

Protect assigned user ID and passwords to avoid unauthorized use by others

- Keep your passwords private - do not share them with others
- Do not use other's login and password to logon to Corewell Health resources
- Keep your passwords safe - never put passwords in electronic documents or Oulook contacts; if you need to write passwords down keep them under lock and key
- Use unique passwords across applications and websites
- Keep your username and passwords secure - do not login to websites if you clicked a link in an email - this could be a malicious actor trying to obtain your credentials
- If you visit a website and a pop-up asks you to enter your username or password, if unsure, don't provide

Appropriate Software, Media and Internet Use

Refer to the **Acceptable Use Policy** for more information.

Service Desk: 888.481.2448 (East) | **269.428.2005** (South) | **616.391.4357** (**1-HELP**) (PH/West)

Lost or Stolen Devices

Team members must report lost or stolen devices immediately to the Service Desk if they meet the following criteria:

The device is owned by Corewell Health

The device contains any Corewell Health data
- This includes any personal device such as a mobile phone/device that contains Corewell Health email or documents

Service Desk:
East: 888.481.2448 | South: 269.428.2005
PH/West: (616.391.4357 or 1-HELP – option 3, option 1)

Phishing Threats

The term 'phishing' is taken from the word 'fishing.'

Much like fishing, 'phishing' is when cyber criminals try to lure people into clicking a link or opening an attachment in an email that will either download malware or steal sensitive data.

Signs of a Phishing Email:

- Impersonal greeting
- Unrecognized senders email
- Unsolicited link/file
- Punishment/fear/urgency
- Poor grammar
- Promoting offers or solutions for current local, national or global issues

What do phishers want?

- Bank information
- Credit card information
- Usernames and emails
- Passwords
- Personal information
- Medical records
- Access to other team members or executives
- Health plan data
- Company financial records
- Patient or health plan member information

Vishing – Be Aware of Malicious Phone Calls

What is vishing? This is when people receive phone calls from malicious actors who are trying to get sensitive information from them over the phone.

Callers pretend to be representatives of valid companies such as Microsoft, Apple, business partners and vendors or even Corewell Health.

Phone numbers can be "spoofed" to appear to come from government agencies such as the IRS, FBI, DEA or even licensing bodies such as LARA.

Never confirm your employment, give out financial information or share sensitive or personal data if the caller sounds suspicious.

Report to your leader and the Service Desk if you are unsure of the caller. Feel free to tell the caller you will have to call them back. Click **here** to learn more.

Have Questions? Contact Information Security at:

Service Desk:
East: 888-481-2448
South: 269-428-2005
PH/West: 616-391-4357 (1-HELP)

Visit Information Security

Choose the Contact Information Security tile on The Well to request assistance with Security Questions –
Corewell Health Employee Center

Safeguarding Sensitive Data

All related policies and procedures are available online through PolicyTech

Corewell Health™

Partner | Educate | Advise

Priority Health™

Safeguarding Confidential and Sensitive Data

Confidentiality, Intellectual Property, and Data Classifications

Care must be given when using, storing, discussing or transmitting information (verbal, written, or electronically) that may put our competitive advantage, business strategy, methods, process, and proprietary business information at risk. Safeguarding sensitive and proprietary business information from improper disclosure is the right thing to do and the responsibility of all team members.

Review the **Data Classification Standard** and the **Professional Expectations Policy**.

Restricted and Confidential Information include Protected Health Information (PHI), Personally Identifiable Information (PII), proprietary information and intellectual property. Store it safely, share only with those authorized and discard it according to applicable procedures.

Business partner information must be protected as we would Corewell Health information. We must understand restrictions regarding its use and only allow it to be accessed by others for legitimate business. If we share confidential information, we must ensure everyone agrees to maintain confidentiality.

Keep trade secrets and intellectual property safe. Share only with others who are authorized to receive and do not accept others' trade secrets or use copyrighted information without permission.

Improper handling of sensitive information can result in breach of contractual, legal or regulatory responsibilities or financial loss. Data exposure threatens the health and reputation of our organization.

We all must safeguard sensitive data properly!

Questions about data use or handling, contact **information governance**.

Questions about intellectual property or copyright laws, contact legal or refer to policies.

Protecting Corewell Health

Corewell Health holds various forms of sensitive and confidential data. It is important to safeguard your data and devices.

To protect this data you must:

- Only use approved tools such as Haiku, Canto or PerfectServe to capture patient PHI or patient photos. EPIC or Microsoft apps can be used to document patient notes. Use EPIC Secure Chat (South/West) or Mobile HeartBeat (East) for any patient care communication.
- Use Corewell Health approved email addresses or instant messaging tools for job duties. Never use personal email addresses, instant messaging tools or texting on personal devices.
- Do not take business assets or data off-site unless you are approved to do so, and your role requires it. Always secure your laptop.
- If you need to dispose of media containing sensitive data, contact the Corewell Health Asset Management Department for assistance.

If you have any concerns about sensitive/confidential data contact information governance by email or contact the Service Desk. Report all lost or stolen devices (even personal devices with access to Corewell Health resources) to the Service Desk immediately (24/7).

East: 888.481.2448 | **South:** 269.428.2005 | **West:** 616.391.4357 or 1-HELP

Artificial Intelligence (AI) Use at Corewell Health

Generative Artificial Intelligence (AI) refers to tools that can generate new and original content like text, images, and audio. These AI tools, such as ChatGPT, can produce false information, perpetuate human bias, or can add sensitive information to the public domain.

To ensure we are using AI responsibly, Corewell Health has an Artificial Intelligence Center of Excellence (AI COE). The AI COE oversees the process for onboarding and monitoring AI technologies for use at Corewell Health.

Team Member Responsibilities

To do the right thing, we must all:

- safeguard Corewell Health's sensitive data
- consider ethics and fairness with AI use
- submit AI use cases to the AI COE for review
- follow the **AI Tools Policy**, which says in part: *Team members may not use publicly available AI Tools **on either a Corewell Health computing device or personal device** for any Corewell Health purpose unless approved by the Artificial Intelligence Center of Excellence (AI CoE).*

Responsible use of AI at Corewell Health will improve the experience for our patients and health plan members. **Artificial Intelligence: Center of Excellence**

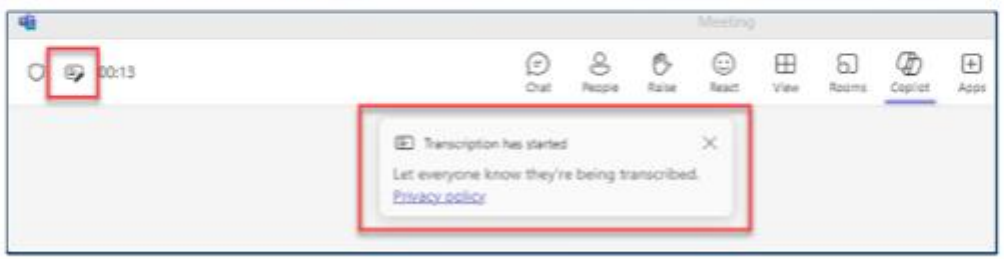
Teams Meetings Best Practices

Safeguarding our data is so important. It protects our patients and health plan members, keeps us compliant with laws and regulatory requirements and allows us to build and maintain trust with the communities we serve.

- Decide if you need to record or transcribe the meeting by considering the purpose, audience, and sensitivity of the meeting content. Recording a meeting may not be necessary or appropriate for every meeting.
- Notify the meeting attendees that you are recording/transcribing the meeting and include a notification in the meeting's chat for those who join late. Meeting recordings and transcriptions can be turned off at any time.
- Do not record/transcribe sensitive discussions or sensitive information.

How to identify if a meeting is being recorded/transcribed

As a meeting attendee, you have visual cues to determine if a meeting is being recorded or transcribed in a Teams meeting room.



When in doubt, don't transcribe or record!

Protecting Credit Card Data

Corewell Health handles payment card (credit or debit card) data for patients, health plan members and team members (billing, gift shops, cafes, etc.).

To comply with the Digital Payments Security Standard and the Compliance Security and Payment Card Processing Standard, **we must all protect this data:**

- Inspect card readers in your area for tampering or unauthorized device substitution
- Payment card numbers should not be stored on paper, Word documents, or Outlook contacts
- Payment card numbers should not be mailed, messaged, faxed, or emailed
- Patient/health plan member card information should never be shared
- Use only approved card entry devices

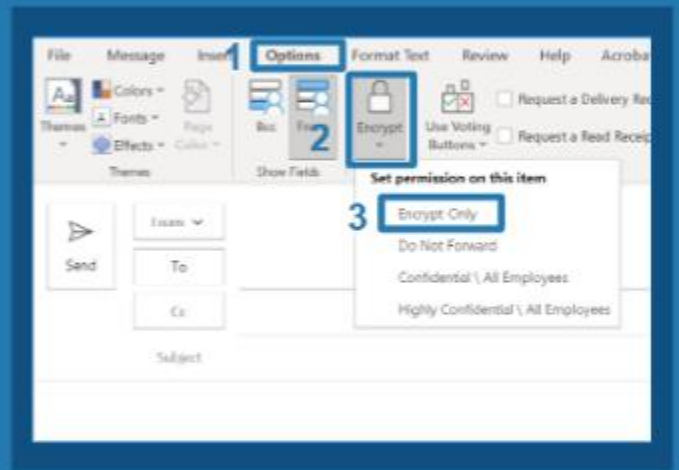
For more information, click **here** to visit the Information Security PCI Homepage.

Digital Payments Security Standard

Pause Before You Send Email

To avoid sending PHI to unauthorized individuals, please consider these tips:

- **Encrypt:** If sending a request for sensitive information (outside of Corewell Health) your email must be encrypted. PHI or PII cannot be included in a subject line.
- **Review before Sharing:** Be sure any attachments or content in an email is necessary for all recipients before forwarding.
- **Check for Minimum Necessary:** Limit PHI and PII to what is necessary to complete the job function and only include those who need to know, especially when forwarding.



Storing Sensitive Data

Do not store sensitive data on unapproved cloud services, public network drives or unapproved devices (e.g. personal devices).

Key Takeaways on Social Media

When you use social media, the following recommendations should be helpful.

NOTE: Encourage team members to report any potential HIPAA violations on social media that affect Corewell Health.

Social Media Policy

1. **Never share PHI/patient/health plan member information** on social media. Even de-identified information or images can be considered PHI if accompanied with other data that could be used to identify an individual.
2. **Do not share photographs/videos** of patients or health plan members without proper authorization or consent forms.
3. **Do not share, post** or otherwise publish any information, including **images** or **recordings**, that you have **obtained as a result of your professional relationship** with a patient or health plan member.
4. **Do not interact with any posts** the patient or health plan member makes **about the medical conditions they have**.
5. **It is not recommended to friend** or follow **patients or health plan members** on social media sites.

Key Takeaways for Safeguarding Sensitive Data

Sensitive data (physical or electronic) containing Protected Health Information (PHI) or Personally Identifiable Information (PII) must be protected.

Protect PHI from others even at home or in public.

Do not share login or password information or badge access.

Shield computer screens from others' view.

Lock/log off computer when not in use.

Only access sensitive information (PHI, PII) to do your job duties.

Do not use personal email for work purposes and do not access on organizational devices.