Corewell Health™

Compliance Education

REVISED 10/15/2025

01

Compliance Program

What is a Compliance Program?

Corewell Health™

A compliance program safeguards an organization's legal responsibility to abide by applicable laws and regulations. A compliance program also helps an organization live its values and ethics.

Our compliance program is aligned with the **Seven Elements of an Effective Compliance Program.**

What does this mean at Corewell Health?

Seven elements of an effective compliance program	How our compliance program meets the element requirements
1. Implementing standards of conduct, policies and procedures	Our Code of Excellence sets clear expectations. Policies and Procedures are integral to our operations and essential tools to help detect, prevent and correct potential compliance issues.
2. Establishing compliance oversight	Compliance Officers and Board of Directors through their Compliance Committees implement, monitor and oversee the compliance program.
3. Conducting effective training and education	Education is provided to ensure knowledge of federal, state and local regulations, accreditation standards and contractual obligations to assist in addressing key risk areas.

What does this mean at Corewell Health?

Seven elements of an effective compliance program	How our compliance program meets the element requirements
4. Developing effective lines of communication	Compliance is here as a resource and partner. Our Integrity Help Line is managed by an independent vendor and is available 24/7.
5. Conducting internal monitoring and auditing	Performing planned audits, onsite visits, interviews and routine monitoring help identify emerging risks as well as resolve issues in previously identified areas.

What does this mean at Corewell Health?

Seven elements of an effective compliance program	How our compliance program meets the element requirements
6. Enforcing standards through disciplinary guidelines	The compliance department in conjunction with human resources establishes standardized guidelines for a fair and consistent approach to managing performance and conduct issues.
7. Investigating and remediating issues	All reports of concerns or issues are reviewed and investigated by the compliance department and other partnering departments who collaborate throughout the process to ensure each report is resolved.

Corewell Health Code of Excellence

Our Commitment to Ethics and Integrity

- What we do matters. As a health system, we can **improve health, instill humanity and inspire hope**. How we go about fulfilling our mission also matters.
- Our Code of Excellence sets clear expectations for how we act and make decisions every day. The core principle of our Code is: **We do the right thing.**
- Doing the right thing means we speak and act in accordance with our values. When we're unsure of what's right, we ask for help. When there are different ways to achieve the right outcome, we seek to make the best decision possible, guided by our values and knowledge. We do the right thing even if no one notices or is watching and even if it's not the easy thing to do.
- By embracing and living this Code, each of us contributes to a culture of trust and transparency, innovation and continuous improvement, compassion and generosity. Each of us helps establish our system as one that welcomes all, encourages everyone to contribute, and is dedicated to solving the tough issues our patients and health plan members' encounter.

Mission
Improve health, instill humanity and inspire hope.

Vision
A future where health is simple, affordable, equitable and exceptional.

Values
Compassion. Collaboration. Clarity. Curiosity. Courage.

Corewell Health Code of Excellence

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 follow the highest standards of ethics and integrity.** 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.
2. **We make sure everyone has a voice.** We raise concerns and evaluate them in a fair and just manner. 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 serve everyone in our communities, without regard to race, color, sex, national origin, 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 prioritize team member wellbeing and foster belonging.** We promote a positive, supportive environment where each team member feels valued and included. We act in safe and healthy ways and perform our duties with clarity and focus.
5. **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.
6. **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 from a government health care program, commercial payer, or patient.
7. **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.
8. **We protect the 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.
9. **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.

Corewell Health™

02

Fraud, Waste and Abuse

Fraud, Waste and Abuse

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**.
- **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 actions but rather by the misuse of resources.
- **Abuse**: **ABUSE** generally occurs when there is no intent to deceive but the situation will still result in unnecessary or inappropriate care or related services.

Laws Governing Fraud, Waste and Abuse

Corewell Health™

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

- *False Claims Act (FCA)
- Anti-Kickback Statute
- Stark Law

- Social Security Act
- The United States Criminal Code
- *Deficit Reduction Act

*We will focus on the Deficit Reduction Act and the False Claims Act.

Corewell Health™

03

Deficit Reduction Act / False Claims Act

What is the Deficit Reduction Act?

The Deficit Reduction Act of 2005, is multifaceted. The section of the act we will focus on is related to the three provisions that target Medicaid program integrity and fraud and abuse.

- First, it provides Center for Medicare and Medicaid Services (CMS) with funds to fight fraud, waste and abuse.
- Second, it created incentives for states to implement fraud and abuse laws that mirror the federal law.
- Third, it requires any entity that receives or makes payments to the State Medicaid program of at least $5M annually, provide training regarding the federal and state false claims laws, and related qui tam/whistleblowers provisions to all team members, contractors and agents.

False Claims Act

What is the False Claims Act?

The federal False Claims Act, also known as Lincoln's Law, was initially passed during the Civil War to control fraud that was occurring with military funds. It is now used to fight fraud in ANY federally funded contract or program, such as Medicare and Medicaid.

Activities Covered by the False Claims Act

Corewell Health™

- Knowingly presenting (or causing to be presented) to the federal government a false or fraudulent claim for payment.
- Knowingly using (or causing to be used) a false record or statement to get a claim paid by the federal government.
- Conspiring with others to get a false or fraudulent claim paid by the federal government.
- Knowingly using (or causing to be used) a false record or statement to conceal, avoid or decrease an obligation to pay money or transmit property to the federal government.

Penalties / Liabilities for Violating Fraud, Waste and Abuse Laws and Regulations

Corewell Health™

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

04

Whistleblowers

Rewards for Whistleblowers

Corewell Health™

If the lawsuit is successful, the whistleblower may receive an award ranging from 15-30% of the amount recovered.

The whistleblower may also be entitled to reasonable expenses, such as attorney fees.

If a court finds that the whistleblower planned or initiated the false claims, the award may be decreased. If the whistleblower is convicted of crimes related to the false claims, no award will be given.

Blowing the Whistle

A whistleblower is a person who ***reports in good faith*** information or activity they believe to be a violation of a law, rule or regulation.

Using the “qui tam”-provisions that are a part of law, any person may file a lawsuit on behalf of the government in federal court.

Once filed, the lawsuit is kept confidential or “under seal” while the government investigates the allegations and decides how to proceed.

If the government decides that the lawsuit has merit, it may intervene. If this is the case, the U.S. Department of Justice will try the case.

The government may decide not to intervene. In this case, the whistleblower would have to continue with the lawsuit on his or her own.

Whistleblower Provisions

Retaliation against someone who files a False Claim Act lawsuit, or tries to stop or prevent a False Claim Act violation, may be entitled to additional relief;

- Including reinstatement of employment
- Back pay
- Compensation for costs and damages

Non Retaliation

Corewell Health prohibits retaliation directed toward a person who is involved in:

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

Any individual who commits or condones any form of retaliation is subject to appropriate corrective action including termination of contract and / or loss of access to Corewell Health systems.

If you believe that retaliation has occurred report it to the compliance department or the Integrity Help Line at 1-877-319-0266.

Reporting your Concerns

Corewell Health™

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 you report?

- Talk to your contact at Corewell Health
- Compliance department
- Integrity Help Line

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

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

Corewell Health™

05

Privacy / Information Security

What is HIPAA and the Privacy Rule?

Corewell Health™

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was created to protect the privacy of an individual's health information while at the same time permitting needed information to be disclosed for patient care and other purposes.

There are two rules for HIPAA: the **HIPAA Privacy Rule** and the **HIPAA Security 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).

It requires safeguards to protect the privacy of PHI and controls use and disclosures that can be made without patient authorization. Also, it gives patients certain rights to their health information.

*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 (HHA) has adopted standards.

Protected Health Information

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 (HHA) has adopted standards.

What are the 18 Patient Identifiers?

Corewell Health™

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 3 patient identifiers** to identify patients.

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 for your job.

- ✓ 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** corrective action including termination of contract and / or loss of access to Corewell Health systems

Permitted uses for PHI

Corewell Health™

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

Confidentiality

Corewell Health™

Patients expect that their confidentiality is maintained, and this is enforced by HIPAA

When accessing information, be sure you are only using the minimum necessarily needed to complete your job functions.

Never access your own information (access only through MyChart)

Never access the records of friends or family for reasons outside of TPO purposes. Curiosity and caring are not acceptable reasons to access a patient record. If you are not the care provider for an individual, do not access their information. It is recommended you recuse yourself from patient care involving family members when possible.

Discussing or sharing patient information outside of TPO purposes is a violation of HIPAA and policy. This also includes social media. Never share any information gained through your relationship with the patient on social media. Even in the case of de-identified information, comments from your or your colleagues may lead to inadvertent identification of the individual making the post a breach of privacy.

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 department / TPO purposes

What if 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 are accountable for their actions and PHI access under their login. Inappropriate access to PHI, regardless of intent, can **result in** corrective action including termination of contract and / or loss of access to Corewell Health systems.

HIPAA Security Rule

Corewell Health™

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

Specifically, we must:

- Ensure the confidentially, 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 all individuals are required to follow to ensure that day-to-day operations and interactions with digital systems are secure.

Guidelines for Use of Social Media

Corewell Health™

If you are going to use social media, the following recommendations may be helpful.

1. **Never share PHI / health plan member information** on social media. Even de-identified information or images an 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.

Secure your Workspace

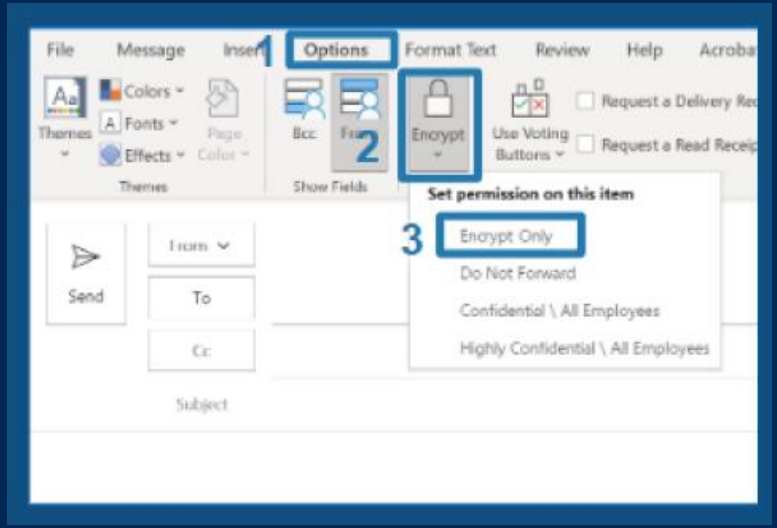
Physical access is the quickest way for someone to get information.

- Do not leave computers / patient files / sensitive data unlocked (Log out with Windows Key + LOR approved department logout procedures) **even when working from home.**
- Securely store personal devices or carry them on you.
- Properly store or dispose of all papers in a secure manner.
- Be aware and suspicious of unknown individuals in secure areas.
- Create strong passwords, don’t share or reuse them.
- It is a violation of policy to share passwords with anyone.

Protecting Sensitive Data

To avoid sending PHI to unauthorized individuals, 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. devices).

Protecting Company Data and Assets

If you are assigned a portable device, or if you are authorized to use a personal device to check Corewell Health resources such as email, you need to review the policies for these devices.

Portable devices such as laptops, tablets and smartphones are often stolen for the data they contain, so it is important to safeguard them.

To protect data, you must:

- If you are backing up confidential information to a USB drive, optical storage device, memory care, flash card or CD / DVD, it must be encrypted and kept in a secure location when it is not being used.
- Do not take any business assets or data off-site unless your role requires it and you have permission.
- Do not leave your laptop unattended or unsecured if you are outside the office.
- Install appropriate applications to portable devices to decrease the risk of exposure of PHI or PII.

Report all lost or stolen devices (even personal devices with access to Corewell Health resources) to the DS Service Desk at 616.391.4357 or **1-HELP** immediately (24/7) and contact the security services personnel.

Acceptable Use Policy

For any other information on use of Corewell Health assets or access of data, please familiarize yourself with the Corewell Health Acceptable Use Policy and its associated standards.

Protecting Credit Card Data

Corewell Health

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

Phishing Threats

Corewell Health™

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

Report Phishing

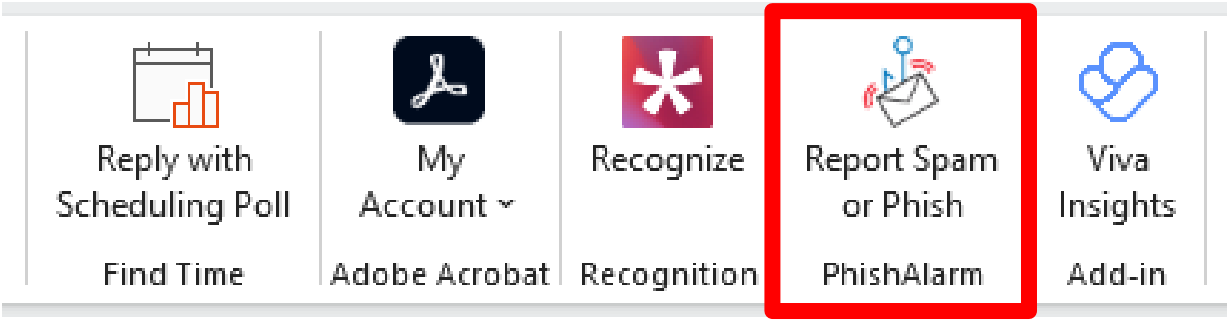
Corewell Health™

If you suspect phishing:

- Do not click links
- Do not download attachments
- Do not respond
- Do not forward to others in your department

Click the Report Spam or Phish button and confirm the action by clicking Close. The message will automatically be moved to the Outlook Deleted Items folder.

Any message classified as malicious will automatically be removed from Outlook. If a message is determined to be safe, it will be restored to the individual's mailbox.



Privacy and Information Security Contacts

Privacy Team: privacy@corewellhealth.org

Privacy Hotline: 616-486-4113

Corewell Health DS ServiceDesk:
Corewell Health East: 888-481-2448
Corewell Health South: 269-428-2005
Corewell Health West: 616-391-4357 (1-HELP)