Corewell Health™

Compliance Education

REVISED 10/01/2024

Corewell Health™

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.
An effective compliance program also helps an organization live its values and ethics.

Our **Compliance Program/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.**

Seven Elements of an Effective Compliance Program… What does this mean at Corewell Health?

Seven Elements of an Effective Compliance Program	How our Compliance Plan 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	We empower team to do the right thing by providing education to ensure knowledge of federal, state and local regulations, accreditation standards and contractual obligation to assist in addressing key risk areas.

What does this mean at Corewell Health?

Seven Elements of an Effective Compliance Program	How our Compliance Plan meets the element requirements
4. Developing Effective Lines of Communication	Compliance leaders are here as a resource and partner for you. We provide third party reporting through our Integrity Help Line, 24/7 with an anonymous reporting option.
5. Conducting Internal Monitoring and Auditing	Performing planned audits, onsite visits, interviews and routine monitoring helps identify emerging risks as well as resolved issues in identified areas.

What does this mean at Corewell Health?

Seven Elements of an Effective Compliance Program	How our Compliance Plan meets the element requirements
6. Enforcing Standards Through Disciplinary Guidelines	The compliance department in conjunction with human resources established 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 compliance department partners who educate throughout the process to ensure each report is resolved.

Corewell Health™

02

Fraud, Waste and Abuse

Fraud, Waste and Abuse

Each of use 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 services 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 not intent deceive.

Laws Governing Fraud, Waste and Abuse

Corewell Health™

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

- **False Claims Act**
- 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 False Claims Act.

Corewell Health™

03

Deficit Reduction Act

What is the Deficit Reduction Act?

Corewell Health

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 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, and most related to us here at SH, it requires that any entity that receives or makes payments to the State Medicaid program of at least $5M annually to provide their employees, contractors and agents training regarding the federal and state false claims laws and related qui tam/whistleblowers provisions.

Corewell Health™

04

False Claims Act

False Claims Act

Corewell Health

What is the False Claims Act?

The Federal False Claims Act (FCA), 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, for us Medicare and Medicaid.

Activities Covered by the False Claims Act

- 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 FWA Laws and Regulations (False Claims)

Corewell Health™

Corewell Health™

05

Whistleblower Protection Act and Non-Retaliation

Whistleblower Protection Act / Non-Retaliation

Corewell Health™

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.

Corewell Health™

06

Privacy / Information Security

What is HIPAA and the Privacy Rule?

Corewell Health

The education in this section will explore and define mandatory policies and best practices to remain compliant with HIPAA regulations for both the **Privacy Rule** and the **Security Rule**.

What is HIPAA?

Corewell Health™

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.

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 (HHA) has adopted standards.

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

What are the 18 Patient Identifiers?

Corewell Health™

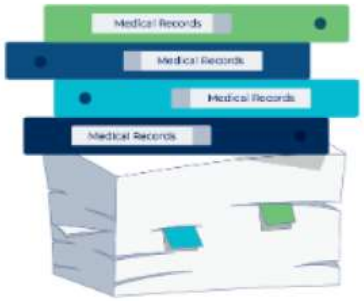
1. Names
2. All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death
4. Phone numbers
5. Fax numbers
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 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

Confidentiality

Corewell Health

Patients and health plan members expect that their confidentiality is maintained, and this is enforced by HIPAA.

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

Never access the records of friends or family for reasons outside of Treatment, Payment, or Operation (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.

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/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.

Auditing and Monitoring

Corewell Health™

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

Corewell Health

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.

Secure your Workspace

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

- Do not leave computers / patient files / sensitive data unlocked (Log out with Windows Key + L OR 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 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 this data you must:

- If you back up confidential information to a USB drive, optical storage device, memory card, 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 and you have permission
- Do not leave your laptop unattended or unsecured, especially if you are outside the office
- Install appropriate applications to portable devices to decrease the risk of exposure of Protected Health Information (PHI) or Personally Identifiable Information (PII)

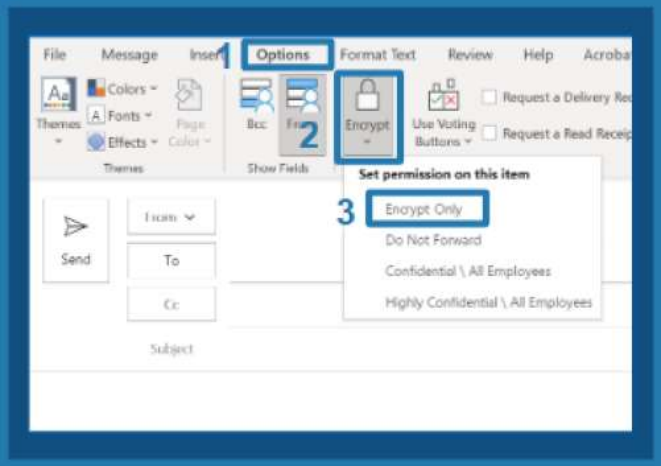
Report all lost or stolen devices (this includes personal devices with access to Corewell Health resources) to the IT Service Desk at 888.481.2448.

Protecting Sensitive Data

Corewell Health™

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).

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

For more information, visit Information Security PCI Homepage

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?

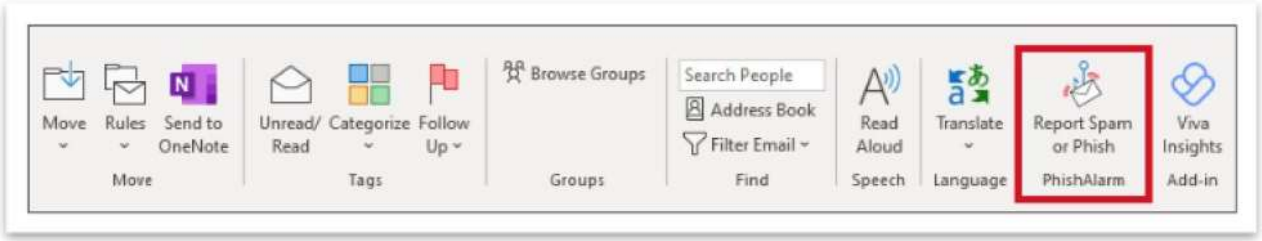
- Bank information
- Credit card information
- Usernames and emails
- Passwords
- Personal information
- Medical records
- Access to other team members or executives
- Health plan data
- Company financial records
- Patient or health plan member information

Report Phishing – Desktop Access

Corewell Health

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 team member's mailbox.



If you suspect phishing:

- Do not click links
- Do not respond
- Do not download attachments
- Do not forward to others in your department
- DO Report Spam or Phish using the button shown above

Report Phishing – Web Access

Corewell Health

Click the **three dots** in the upper right-hand corner of your message.
In the list of choices, click **Report Spam or Phish** and confirm your selection.
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 team member's mailbox.

If you suspect phishing:

Vishing – Be Aware of Malicious Phone Calls

Corewell Health™

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.

Corewell Health™

06

Reporting – Integrity Help Line

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 in 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)

Compliance and Privacy Contact Information

Corewell Health™

Privacy Team
privacy@corewellhealth.org

Privacy Hotline
616-486-4113