Accessible Transcript

Introduction

Welcome to Highmark Health's annual 2023 Compliance, Information Security, and Privacy training. This course will review the key compliance topics that are of significant operational importance across the Highmark Health organization.

Course Navigation

You are responsible for ensuring your understanding of the content included in this course.

Several sections of this course begin with a test-out option. If you answer all quiz questions correctly, you can skip to the next section of the course. If you do not answer all questions correctly, you must review all content found in the subsequent section.

For those learners who need an alternate testing activity, submit an HR Service Request, Subject: ELD 2023 Annual Compliance, Information Security, and Privacy course Alternate Activity.

Please include the following language in your request: "I am requesting support through HR Services to complete my 2023 Annual Regulatory training with an alternate activity. Please contact me with instructions."

The instructions will include how to submit the Attestations required for course completion.

See the Resources within each section of this transcript for all policies, intranet sites, and documents that are referred to in the content. If you have questions about the terms or laws discussed in this course, refer to the Appendix section.

Objectives

At the end of this course, workforce members should:

1. Know what documents and resources are available to help navigate our Compliance, Security, and Privacy Program.
2. Know how to report compliance, privacy and/or security violations.
3. Understand Highmark Health's expectations for ethical business conduct.
4. Learn how to detect and prevent fraud, waste, and abuse.

Know what steps to take to protect Highmark Health's information.

For Allegheny Health Network (AHN) workforce members, note that while you are a workforce member of AHN, you are a member of the Highmark Health family. As a member of that family, references to Highmark Health throughout this course apply to you.

At the end of this course, AHN workforce members should:

1. Know what documents and resources are available to help navigate our Compliance, Security, and Privacy Program.
2. Know how to report compliance, privacy and/or security violations.
3. Understand Highmark Health's expectations for ethical business conduct.
4. Know what steps to take to protect Highmark Health's information.
5. Learn how to detect and prevent fraud, waste, and abuse.

Committing to Integrity and Compliance

Highmark Health's family of companies are committed to creating a remarkable health experience for our customers.

We can only fulfill this promise if our workforce members commit to the highest standard of ethical conduct and work with integrity.

Our customers and our patients are relying on us to do what is good and right, every day. We can meet their expectations by ensuring compliance with established laws, policies, procedures, standards, and by conducting our business ethically.

As a member of the Highmark team, you have a moral duty to behave ethically and work with integrity. You also have a legal obligation to comply with the rules that govern our business. In doing so, we're all winners!

Integrity and Compliance Program Elements

Our workforce is aligned under the Highmark Health Integrity and Compliance program, which provides the framework and the guideposts to ensure we meet our ethics and compliance objectives.

The federal government has identified seven elements of a highly effective compliance program. Highmark Health has added an eighth element to increase our effectiveness. Review each of the elements for additional information.

1. Policies, Procedures, and Standards of Conduct.

Compliance policies and procedures describe the particulars of the Integrity and Compliance Program's operations.

Each Highmark Health organization has its own set of corporate polices, and many departments throughout our organization have their own set of rules called 'departmental policies'. Policies and procedures outline the black and white or the 'dos and don'ts' of our organization.

The Code of Business Conduct defines our organizations' ethical standards and deals with 'the grey areas'. Think of it as the ethical blueprint of the organization. The Code states the overarching principles and values by which the organization operates. There is also a Third-Party Code for contingent workers and other contracted staff at Highmark Health.

The Code of Conduct is updated on an annual basis and approved by the Board of Directors. Workforce members must attest that they have received, read, understand, and agree to abide by the Code upon hire and annually thereafter.

2. Compliance Officer, Committee, and High-Level Oversight.

Highmark Health designates a chief compliance officer for the Highmark Health enterprise, a government (Medicare) compliance officer for Highmark Inc., and a corporate compliance officer for Allegheny Health Network.

The enterprise also has a compliance committee that is accountable and responsible for the activities and status of the compliance program, including the issues identified, investigated, and resolved by the compliance program.

Highmark Health's senior management and Board of Directors are engaged with, and exercise reasonable oversight of the compliance program.

3. Effective Training and Education.

The following oversight agencies require Highmark Health companies to provide effective training and education to its Board of Directors, senior management, and workforce members at the time of hire, annually thereafter, and occasionally throughout the year when circumstances require additional specialized refresher training.

- Centers for Medicare and Medicaid Services (CMS)
- United States Department of Health and Human Services (DHHS)
- Joint Commission
- Occupational Safety and Health Administration (OSHA)
- Pennsylvania Insurance Department
- Various other state agencies

As a condition of employment and/or direct affiliation with Highmark Health, all parties must complete required compliance training.

4. Effective Lines of Communication.

Highmark Health's confidential lines of communication provide you with methods for anonymous and good-faith issue reporting if you suspect or detect unethical conduct, noncompliance, fraud, waste, or abuse. All inquiries and reports are handled in a confidential manner, subject to limitations imposed by law.

If the individual wishes to remain anonymous, the individual should contact the Enterprise Risk and Governance Division. Highmark Health maintains a reprisal-free environment and has a policy of non-retaliation and non-intimidation to encourage workforce members to raise compliance, ethical or legal concerns in good faith.

5. Well-Publicized Disciplinary Standards.

All Highmark Health organizations enforce their standards through well-publicized disciplinary guidelines that are designed to provide a structured corrective action process to improve and prevent recurrence of unlawful and unethical behavior and/or performance issues. Failure to comply with established integrity and compliance policies, procedures and the Integrity and Compliance Program will be treated as a breach of corporate policy and will result in appropriate disciplinary action, up to and including termination.

These disciplinary standards can be found within each policy on PolicyWeb.

6. Effective System for Routine Monitoring, Auditing, and Identification of Compliance Risks.

Risks change and evolve with changes in the laws and regulations, CMS requirements, and operational matters. Our process for monitoring, auditing, and identifying compliance risks includes:

- Internal and external audits of our employed workforce and third-party entities.
- Monitoring activities - which are regular reviews performed as part of normal operations to confirm ongoing compliance and to ensure that corrective actions are undertaken, effective and consistent.
- Ongoing risk assessments.
- A monitoring and auditing work plan that addresses compliance risks.

Our organization must allow access to any auditor acting on behalf of the federal government or CMS to conduct an on-site audit, including interviews of the staff. Workforce members are required to fully cooperate with internal or external audits and inquiries made by the Chief Compliance Officer or the Enterprise Risk and Governance Division. Direct any questions on this process to your manager or the Enterprise Risk and Governance Division.

7. Procedures and System for Prompt Response to Compliance Issues.

Highmark Health must use effective measures to respond promptly to non-compliance and undertake appropriate corrective action. The Enterprise Risk and Governance Division will investigate all allegations in a timely manner and ensure that the proper parties are notified when appropriate.

Highmark Health has implemented procedures to respond to compliance issues as they are raised. Corrective Action Plans are executed as appropriate to ensure corrective action initiatives are taken, implemented, and the detected offenses are corrected. This method tracks and documents the correction of any underlying problems and helps to prevent future issues.

Any workforce member approached by people representing themselves as government investigators must immediately notify the Highmark Health Law Office and the entity Compliance Officer.

8. Ongoing Evaluation of the Effectiveness of Each Element of the Integrity and Compliance Program.

Centers for Medicare and Medicaid Services (CMS) standards for an effective compliance program only include the previous seven elements. Highmark Health has added an eighth element to its enterprise-wide Integrity and Compliance Program to further strengthen our organizations' ability to ensure compliance with the law.

Through this element, Highmark Health evaluates the effectiveness of the program to ensure that it is working properly.

Remember, all Highmark Health, AHN, and Enterprise policies and procedures can be accessed through PolicyWeb.

Conflicts of Interest

Avoid Conflicts: Doing what's good and right for our customers and patients means avoiding conflicts of interest.

Be Conflict Free: Highmark Health requires all individuals of any of its subsidiaries', Boards of Directors ("Directors"), officers, and workforce members to remain free from any conflict of interest that may hinder their ability to perform their responsibilities objectively, effectively, and fairly.

Understand When You May Have a Conflict: A conflict of interest is a competition between your personal private interests and your job responsibilities.

Perception of a Conflict is a Problem: Conflicts of interest or the perception of a conflict are easily resolved by working with your manager and the Enterprise Risk and Governance Division to develop a plan to manage your competing interests.

Familiarize Yourself with the Conflict of Interest Policy which can be found on PolicyWeb.

Enterprise Records Management

Managing records is another way you can commit to compliance and show integrity by protecting the personal data of our members.

Let's review all of the types of records we have in our organization and think about the guidelines you need to apply in your role. See the Enterprise Records Management Policy for further guidance.

Official Record

Official records document and provide evidence of business transactions and the meeting of legal obligations.

They contain information that has ongoing business or legal value, are required to support operations, are required by laws, regulations, contracts, directives, or have current or future business, financial, or legal value.

Transitory Record

Transitory records are required only for a short time and are not required to meet legal or fiscal obligations or provide evidence of decision-making. Transitory records have no business value that warrants retaining them beyond their moment of immediate usefulness. Drafts, duplicate copies and working papers are considered transitory. Except in cases where these records are subject to a legal hold, these records should be discarded after the purpose for which they were created has been fulfilled.

Physical versus Digital Records

If both a physical and digital copy of a record exist, the digital record shall be considered the official record to be retained while the physical copy shall be deemed transitory. Company records in the form of agreements, contracts, etc. containing “wet-ink” signatures should be preserved in physical form with a digital (e.g., scanned copy) backup. Other potential exceptions to official vs. transitory records classifications must be submitted to the Integrated Risk Operations team in writing for further analysis and disposition. Contact them at: integratedriskandprivacyops@highmarkhealth.org.

Digital Record

Because the digital copy of a record shall be considered the official copy, the volume of material sent to offsite storage should be kept to an absolute minimum. Integrated Risk Operations reserves the right to deny any request to send material to offsite storage if it is deemed unnecessary.

Destroying Records

Under no circumstances whatsoever can any record, paper or digital, be destroyed if it is under Legal Hold, even if it is otherwise past retention.

Consult the Legal Hold microsite for further information.

Record Retention Provision

If a contract contains a records retention provision with designated periods longer than what is listed in the Retention Schedule, the retention length in the contract shall be adhered to with the pertinent documents. For instance, if a contract says a certain type of record must be retained for seven (7) years but the Retention Schedule assigns a five (5) year period, the material should be retained for seven (7) years.

Retention Period

The retention periods listed in the Retention Schedule are to be considered the minimum retention requirements. As the Schedule is an important tool in the Enterprise’s risk management strategy, employees are strongly encouraged to adhere to it as it ensures the Enterprise will always follow applicable laws and regulations and will be minimally exposed to liabilities such as data breaches and subpoenas. However, if a department or team insists upon retaining records for a period longer than the Schedule designates, they should first perform their own risk analysis or work with Integrated Risk Operations in addition to their own risk analysis and RP to determine if the benefits outweigh the risks.

See the Records Retention Schedule in the Enterprise Records Management Policy for more details.

Email Storage

Under no circumstances is email to be used as storage; if an attachment must be retained, please save it to a drive or Teams channel.

What would you do?

Keisha has an in-person meeting scheduled to review next year's budget projections. She has printed all relevant documents to share with the other meeting attendees. Once the meeting is over, what should be done with the printed copy if a digital copy is saved?

The paper records are Official Records and should be boxed and shipped to offsite records storage.
The paper copies are Transitory Records and should be placed in a secure shred bin as the digital copy is considered the Official Record.
The paper records are Official Records and should be placed in a locked filing cabinet until their retention period has passed.

Feedback: The digital copies are considered the Official Records, therefore the paper Transitory Records should be placed in a secure shred bin.

What would you do?

Arlando has received a Statement of Work (SOW) from a third party vendor for new tasks that Highmark has asked them to perform. Once he receives the signed SOW back from his VP and forwarded it to the vendor, what should he do with it?

Delete it, it's no longer needed.
Move it to a special Outlook folder where he saves important records.
Move it to a designated document repository such as a Teams Channel or OneDrive.

Feedback: The SOW should be moved to a designated document repository such as a Teams Channel or OneDrive.

Accessing Policies

Both Highmark Health and Allegheny Health Network's policies can be found on **PolicyWeb**. Note that PolicyWeb can be found in the Digital Hub.

Can't access PolicyWeb? Talk to your manager.

Resources

PolicyWeb: http://policyweb.synergy.local/. Search for:

- Enterprise Integrity and Compliance Program
- Corrective Action Policy
- AHN Corrective Action Policy
- Enterprise Conflicts of Interest Policy
- Enterprise Gifts & Entertainment Policy

Integrity and Compliance Site: Contact Integrity and Compliance by selecting the button on the right or by calling the anonymous reporting hotline at 800-985-1056 (toll free, 24/7), via email at integrity@highmarkhealth.org or integrity@highmark.com, or at the Secure Message Platform at https://www.highmarkhealth.org/hmk/ .

Enterprise Risk and Governance: https://highmarkhealth.sharepoint.com/sites/EnterpriseRiskGovernance

Highmark Health Integrity and Compliance site: https://highmarkhealth.sharepoint.com/sites/IntegrityCompliance/SitePages/Combating.aspx Highmark Health Code of Conduct: https://www.highmarkhealth.org/hmk/pdf/highmarkHealthCodeBusinessConduct.pdf

Highmark Health Third Party Code of Conduct: https://www.highmarkhealth.org/hmk/pdf/highmarkHealthThirdPartyCodeBusinessConduct.pdf

Elements of the Compliance Program: https://highmarkhealth.sharepoint.com/sites/IntegrityCompliance/SitePages/Highmark-HealthIntegrity-and-Compliance-Program.aspx

ER&G Legal Holds: See this Enterprise Risk & Governance microsite for more details about legal holds on document destruction at https://highmarkhealth.sharepoint.com/sites/EnterpriseRiskGovernance/SitePages/LegalHolds.aspx

Email the Integrated Risk Operations Team with questions regarding official vs. transitory records classifications at integratedriskandprivacyops@highmarkhealth.org.

Current Issues

We have identified specific compliance issues that require extra attention from all our Highmark Health workforce members. While we review these current issues, consider the steps you can take to change your actions and habits.

Issue: Phishing Emails and Data Breaches

Cyber security is integral to achieving our compliance goals and maintaining our customers' trust. In the wake of the data breaches we have experienced, it is more important than ever to be vigilant about emails and confidential information. Look for our Cyber Security module in the Protecting Our Information section. This module is required for all workforce members this year because you are the most important line of defense we have.

Issue: Videos and Photographs in our Workplace

Workforce members are not permitted to take photographs or record videos for social media posts within Highmark Health or AHN facilities. These types of social media posts risk the privacy and confidentiality of our patients, our members, and our business.

This includes the use of Snap Chat, Instagram, FaceTime calls, or posting videos to social media platforms such as TikTok.

There is no exception to this rule.

Issue: Accessing Your Own Medical and Claims Records

It may be tempting to look at your own records. It's your information, right? But Highmark Health does not permit you to access your medical/claim records or the medical/claim records of anyone else for non-business needs.

Use the MyChart app to access your own medical records, test results, and future appointments.

Issue: Bullying

Harassment and bullying of co-workers, customers, vendors, or patients is not permitted. The company has a zero-tolerance policy for harassment or bullying. Please refrain from engaging in any type of behavior that can be considered intimidating.

Issue: Theft of Time

The remote work environment provides many of us increased flexibility and improved work-life balance.

Engaging in personal activities, such as working on a second job, online shopping, updating your social media accounts, etc. while being paid to perform your job responsibilities is considered theft of time and is a serious threat to achieving our compliance goals.

You must also abide by the work hours agreed upon with your leader and be available during those times.

Lastly, you are not permitted to use Highmark Health assets to support any business outside of Highmark. This includes sending and receiving non-Highmark business related emails, using software licensed to Highmark Health for anything that doesn't directly benefit our organization, or using printers or other hardware for personal gain or profit.

Issue: Acceptable Use of Information

You created an excellent presentation for your team, and you know it will be a great asset to your work portfolio. You decide to email it to your personal email address. There's no problem, right?

Wrong! Be aware that all work products created for any of the Highmark Health family of companies are the property of Highmark Health and may not be shared outside the organization.

Even if the presentation does not contain protected health information (PHI), company financial information, or information related to our policies and procedures, all information contained in that presentation is considered a work product of our organization and is therefore confidential and may not be shared outside of our company.

Highmark Health has established guidelines for information sharing. You should familiarize yourself with the Acceptable Use of Electronic Communication & Information Policy via PolicyWeb.

Issue: Improper Expense Reimbursement

Many workforce members are responsible for making purchases on behalf of our organization. And many of our workforce members are required to travel based on their job responsibilities. As a result, these workforce members have reimbursable expenses that should be submitted in a timely manner.

It is important to follow the guidelines and only submit expenses that are reimbursable, so that we can reach the high standards we have set for compliance.

We are relying on you to help us raise compliance expectations.

Now, take a few moments to practice with these common scenarios.

What would you do?

John received an email from www.healthathighmark.org stating that he is the recipient of a $100 gift card. The email tells John to click the link to collect the gift card. What should John do?

Click the link and provide the requested information.
Delete the email and do nothing. As long as you don't open any suspicious emails, it should be fine.
Forward the email to phishing@highmark.com so that the email can be investigated.

Feedback: John should forward the email to phishing@highmark.com. If you are suspicious, forward the email.

What would you do?

Your co-worker sent you a picture of their new puppy. You can see their computer screen. Is this ok?

Yes
No

Feedback: No, you should never take a picture of your work computer screen and share the image, even if it is with a coworker.

What would you do?

You joined one of the Highmark challenges and you work out at a gym near your house. You are super proud of how hard you are working, and you snap a selfie while working out and post it to your challenge group page.

Is this a violation of our privacy policies?

Yes
No

Feedback: This use of a photograph and social media is ok! You are at a gym that is not located at a Highmark facility, so you can post your picture to your challenge group page.

What would you do?

Your child recently had tests done, but you still have not received the results from her physician. As a nurse employed by AHN, are you permitted to access her medical records and review her test results using your EPIC credentials?

Yes, you can use your EPIC access to look at your daughter's medical records.
No, you cannot use any internal system to look at your daughter's medical records.

Feedback: No. You cannot use your EPIC or any other internal system access for a non-business purpose. Use your MyChart app.

Resources

PolicyWeb: http://policyweb.synergy.local/

- Corporate Credit Cards
- Business Travel & Employee Expense Reimbursement
- Non-Retaliation
- Recorded Communication
- Enterprise Social Media

HIPAA: https://www.hhs.gov/hipaa/index.html

Data Ethics, Policy, and Privacy Department: https://highmarkhealth.sharepoint.com/sites/Privacy

Data Ethics, Policy, and Privacy Handbook:
https://highmarkhealth.sharepoint.com/sites/Privacy/Shared%20Documents/Forms/AllItems.aspx?id=%2Fsites%2FPrivacy%2FShared%20Documents%2FCS202563%5FPrivacyHandbook%5FBK%5FFFF%5F1%5F11%5F19%2Epdf&parent=%2Fsites%2FPrivacy%2FShared%20Documents

Global Procurement and Payables Site:
https://highmarkhealth.sharepoint.com/sites/GlobalProcurementPayables/SitePages/AccountsPayable.aspx

Complying with Legal and Regulatory Requirements

Let's review the rules. When we talk about rules, we mean the business, health care, privacy and security laws, statutes, regulations, contractual guidelines, and accreditation standards that govern our jobs.

You don't need to be a lawyer or to be an expert on the legal requirements and standards that provide the framework for a blended health care organization like Highmark Health. We have many teams of compliance and legal experts that are here to support you.

However, you are expected to do your part. That means that you must have a general understanding of the health care, privacy, and security rules that govern our company. You must also understand how the rules apply to your role within the organization and know how to comply with each rule.

In this section we will refresh your knowledge of some of the most important laws that affect Highmark Health.

The Laws

Let's review the laws and regulations that apply to our company.

21st Century CURES Act

The 21st Century Cures Act is a United States law enacted in 2016. It authorized $6.3 billion in funding, mostly for the National Institute of Health.

The law is designed to help accelerate medical product development and bring new innovations and advances to patients who need them faster and more efficiently.

Patients have several rights under HIPAA that require a time-sensitive response from AHN, so it is important for you to recognize them when a patient chooses to exercise them.

One of those rights is a patient's Right to Request an Amendment. A patient may ask to change – or 'amend' a diagnosis, a provider note, or other documentation in their medical record. These requests must be referred to Integrated Risk Operations as soon as possible. Integrated Risk Operations will work with the clinician of record to review the patient's request and determine whether the documentation is complete and accurate as written or if an amendment to the record is appropriate. Like other patient rights, AHN is held to strict regulatory timelines and response requirements, so it's important that you refer these requests to Integrated Risk Operations as soon as possible to begin the review process.

Another right under HIPAA is a Right to Access: when a patient or their representative requests a copy of their medical records, AHN must provide those records without undue delay - in some cases the records must be provided almost immediately. For example, the CURES Act Final Rule was issued to strengthen HIPAA's Right to Access. This Rule requires AHN to share information with patients, in many cases, in near-real-time through a patient portal. Failure to comply with timely release, or improperly restricting information from release, places us at risk of 'information blocking' as defined by the Rule.

That means if you receive a request for records, it must be handled as soon as possible, whether it's given to your facility's HIM department or your office's medical records staff for processing. DO NOT DELAY processing a patient's request for records, as a delayed response - or lack of response - could subject our company to significant regulatory fines.

For more information about CURES Act requirements, visit AHN Central.

Affordable Care Act

The Affordable Care Act or ACA increases access to affordable, quality health insurance and provides rights and protections that make health care coverage fairer and easier to understand.

ACA was designed to narrow geographic, economic, racial, and social disparities in health care coverage.

ACA protects Americans with pre-existing conditions and prevents insurers from setting annual or lifetime limits on spending.

ACA is focused on preventive care and ensures plans cover the cost of recommended preventive services.

This law improved care for women and children and expanded Medicaid coverage to low-income individuals and families that previously did not qualify for coverage.

Anti-Kickback Statute

The Anti-Kickback Statute prohibits knowingly and willfully soliciting, receiving, offering, or remuneration (including any kickback, bribe, or rebate) for referrals for services that are paid, in whole or in part, under a federal health care program. This includes the Medicare Program.

Anti-Trust Laws

United States Anti-Trust law is a collection of federal and state government laws that regulates the conduct and organization of business corporations, generally to promote fair competition for the benefit of consumers.

Anti-Trust is mainly a concern between competing hospitals, or scenarios where price fixing is possible.

Debarment: Exclusion Screenings

Companies, such as Highmark Health, that participate in federal health care programs such as Medicare, Medicaid, or other government programs, are prohibited by federal law from entering or maintaining certain relationships with individuals or entities that have been excluded from participation in federal health care programs – also known as debarment.

Highmark Health is diligent in ensuring that we do not violate any laws by performing initial and ongoing exclusion screening reviews of workforce members, board/committee members, volunteers, providers, members, and suppliers using the Office of Inspector General's List of Excluded Individuals/Entities (LEIE) and the System for Award Management (SAM) databases as well as state exclusion lists.

Emergency Medical Treatment and Labor Act (EMTALA)

The Emergency Medical Treatment and Labor Act (EMTALA) covers anyone who comes to the hospital, or who is on hospital property, and requests an examination or treatment of an emergency medical condition for themselves or on behalf of someone else. The law requires Centers for Medicare Services (CMS) participating hospitals, which includes all Allegheny Health Network hospitals, to provide emergency health care treatment to anyone needing it in a nondiscriminatory manner, regardless of the patient's ability to pay. As the name indicates, EMTALA also applies to the treatment of pregnant women and their unborn children.

There are three major obligations every hospital has under EMTALA:

- Provide an appropriate Medical Screening Examination.
- Stabilize the patient.
- Only make appropriate transfers.

Highmark Health has policies and procedures in place to ensure compliance with these requirements.

False Claims Act (FCA)

Also called the 'Lincoln Law' because the bill was signed by President Abraham Lincoln in 1863, this federal law imposes liability on persons and companies (typically federal contractors) who defraud governmental programs. It is the federal Government's primary litigation tool in combating fraud against the Government. The law includes a provision that allows people who are not affiliated with the government, called "relators" under the law, to file actions on behalf of the government (informally called "whistleblowing" especially when the relator is employed by the organization accused in the suit). Persons filing under the Act stand to receive a portion (usually about 15-25 percent) of any recovered damages. Claims under the law have typically involved health care, military, or other government spending programs, and dominate the list of largest pharmaceutical settlements. The United States Department of Justice (DOJ) recently announced that it recovered more than $3 billion in settlements and judgments from False Claims Act (FCA) cases in fiscal year 2019.

The civil provisions of the FCA make a person liable to pay damages to the Government if he or she knowingly:

- Conspires to violate the FCA.
- Carries out other acts to obtain property from the Government by misrepresentation.
- Conceals or improperly avoids or decreases an obligation to pay the Government.
- Makes or uses a false record or statement supporting a false claim.
- Presents a false claim for payment or approval.

Damages and Penalties: Any person who knowingly submits false claims to the Government is liable for three times the Government's damages caused by the violator plus a penalty.

New York State (NYS) False Claims Act: Criminal penalties exist for intentionally submitting a false claim to the Medicaid program, filing a false claim with a government agency, committing a fraudulent act, and/ or engaging in health care fraud.

Violations of the NYS False Claims Act include administrative/ civil penalties of $6,000 to $12,000 per claim and treble damages (three times the amount of the false claim).

The Health Care Fraud Statute states, "Whoever knowingly and willfully executes, or attempts to execute, a scheme or artifice to defraud any health care benefit program shall be fined under this title or imprisoned not more than 10 years, or both." Conviction under the statute does not require proof the violator had knowledge of the law or specific intent to violate the law.

Persons who knowingly make a false claim may be subject to:

- Criminal fines up to $250,000.
- Imprisonment for up to 20 years.

If the violations resulted in death, the individual may be imprisoned for any term of years or for life.

Federal Enforcement and Recovery Act (FERA)

The Federal Enforcement and Recovery Act or FERA is a public law in the United States that enhances criminal enforcement of federal laws, especially regarding financial institutions mortgage fraud, and securities fraud or commodities fraud. FERA makes it easier for the government to prove a violation of the False Claims Act.

Criminal penalties may include fines, imprisonment, or both.

Federal Substance Abuse Rules (FSAR)

Now let's look at look at the information protected by the Federal Substance Abuse Rules, and when you can disclose information.

The Federal Substance Abuse Rules protect the confidentiality of alcohol and substance use patient records which include, but may not be limited to:

- Information that would identify a patient as having an alcohol or substance use disorder either directly, by reference to other publicly available information, or through verification of such an identification by another person.

- Information obtained by an alcohol or substance use disorder program for the purpose of rerating alcohol or substance use, making a diagnosis/prognosis for that treatment, or making a referral for that treatment.

Disclosure of alcohol or substance use disorder records is permitted with:

- Proper patient authorization to disclose alcohol or substance use disorder patient records to third parties, including disclosures to bill insurance companies for payment.
- Disclosures of alcohol or substance use disorder patient records permitted without patient authorization include but may not be limited to disclosures to medical personnel who need the information to treat a condition which poses an immediate threat to the health of any individual and which requires immediate intervention.

When disclosing information in accordance with the law, utilize the Authorization for Release of Confidential Protected Health Information (PHI) form for Alcohol and Substance Use Disorder Records.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 or HIPAA, created greater access to health care insurance, strengthened the protection of privacy of health care data, and promoted standardization and efficiency in the health care industry.

HIPAA safeguards deter unauthorized access to protected health care information. As a member of Highmark's workforce with access to protected health information, you must comply with HIPAA. For more information, visit the HIPAA webpage: https://www.hhs.gov/hipaa.

Damages and Penalties: Violations may result in Civil Monetary Penalties. In some cases, criminal penalties may apply.

Example: A former hospital employee pleaded guilty to criminal HIPAA charges after obtaining protected health information with the intent to use it for personal gain. He was sentenced to 12 months and 1 day in prison. Items or services to a Medicare or Medicaid beneficiary that are apt to influence the beneficiary to seek such reimbursable services from a particular provider.

See HIPAA and Social Security Act for related information and allowable limits.

Health Information Technology for Economic and Clinical Health Act (HITECH)

The Health Information Technology for Economic and Clinical Health Act or HITECH Act includes some significant changes to the HIPAA standard regarding the use and disclosure of protected health information (PHI) and also contains notification requirements in the event of a breach of unsecured data.

HITECH provided incentives for health care providers to transition to Electronic Health Records (EHR). It also added language to HIPAA so that business associates of HIPAA covered entities were complying with HIPAA rules, ensuring that notifications were sent to affected individuals when health information was compromised. HITECH also added tougher penalties for compliance failures.

The HITECH Act also increases the consequences of inappropriate disclosure of protected information by raising the fines for non-compliance and granting State Attorney Generals the authority to enforce HIPAA under the HITECH Act, the United States Department of Health and Human Services is promoting and expanding the adoption of health information technology to create a nationwide network of electronic health records. Its purpose is to improve health care quality, safety and efficiency through the use of electronic health records and adopt health information technology standards and improve privacy and security provisions.

Mental Health Parity and Addiction Equity Act

The Mental Health Parity and Addiction Equity Act of 2008 (MHPAEA) is a federal law that requires the same health insurance coverage for mental health and/or substance use disorder (MH/SUD) conditions as patients would receive for coverage of medical/surgical (M/S) services.

Parity (which means equal or fair treatment) requires insurance companies to administer mental health or substance use disorder benefits in the same way as they administer medical and surgical services, meaning both the quantitative limits (QTLs), such as the visit limits or deductibles, as well as the non-quantitative limits (NQTLs), such as prior authorization requirements and network criteria, must be parallel.

Highmark must comply with MHPAEA as well as State regulations related to mental parity, which requires:

- A method for anonymous and confidential reporting of potential compliance issues as they are identified,
- Training regarding MHPAEA, and
- A policy of non-intimidation and non-retaliation for good-faith participation.

Non-compliance can result in civil monetary penalties, increased damages, and other measures.

For more information, see the Resources in this section of the course for links to MHPAEA information.

Mental Health Parity

The Mental Health Parity and Addiction Equity Act of 2008 (MHPAEA) is a federal law that requires that insurers meet mental health parity standards in areas including:

- Copay
- Deductible
- Number of outpatient visits
- Inpatient days covered.
- Prior Authorization requirements related to mental health / substance use disorder and medical surgical care.

Mental health parity refers to the “equal treatment of mental health conditions and substance use disorders in insurance plans.” This ensures that plans provide equitable financial and treatment coverage of both chronic and medical and mental health conditions. MHPAEA applies to most health plans:

- Self-insured
- Full insured
- Individual health plans (on / off Health Insurance Marketplace)

- Large group plans (private / public) with 50+ employees.

The Patient Protection and Affordable Care Act (ACA) requires small group plans to provide mental health / substance use disorder benefits. Any plan that offers mental health / substance use disorder coverage must comply with MHPAEA.

MHPAEA applies to all mental health / substance use disorder diagnoses that are covered by a health plan; however, a health plan is permitted to specifically exclude some diagnoses but must be contained in your Summary of Benefits (SOB) / Certificate of Coverage.

Highmark must comply with MHPAEA as well as State regulations related to mental parity, which requires:

- A method for anonymous and confidential reporting of potential compliance issues as they are identified.
- Training regarding MHPAEA.
- A policy of non-intimidation and non-retaliation for good-faith participation.

Non-compliance can result in civil monetary penalties, increased damages and other measures.

MHPAEA Protections

MHPAEA requires that insurers meet mental health parity standards in two areas:

- Qualitative Limits
- Non-Qualitative Limits

QTL vs. NQTL

Parity also applies to clinical criteria used by health insurers to approve or deny mental health or substance use treatment. The standard for *medical necessity determinations* – whether the treatment or supplies are considered by the health plan to be reasonable, necessary, and / or appropriate – must be made available to any current or potential health plan member upon request. The reason for denials of coverage must also be made available upon request.

Parity also applies to Non-Quantitative Treatment Limitations (NQTLs). NQTLs are processes, strategies, evidentiary standards, or other criteria that limit the scope or duration of benefits for services provided under the plan. Certain utilization reviews, prior authorization and plan provisions may only be applied to mental health / substance use disorder benefits if they are comparable to or less restrictive than those for medical surgical services.

QTLs can be measured numerically. Health insurers generally cannot impose a financial requirement (such as copays, coinsurance, deductible) or a QTL (such as the number of outpatient visits or inpatient days covered) on mental health / substance use disorder benefits that are more restrictive than the financial requirement or QTL that apply to most – but not all – medical surgical benefits in the same classification.

- QTLs are managed by the Actuarial team.
- NQTLs are managed by ER&G Case Management.
- There are 12 NQTL analyses (4 Pharmacy, 6 Health Services / UM and 2 Provider Network). Each analysis has five steps with support of Policies / Procedures and Job Aides

NQTLs include, but are not limited to:

- Medical management standards limiting or excluding benefits based on medical necessity, medical appropriateness, or based on whether the treatment is experimental or investigative (including standards for concurrent review).
- Formulary design for prescription drugs
- Network tier design
- Fail-first policies or step therapy protocols.

For example: Refusal to pay for higher-cost therapies until it can be shown that a lower-cost therapy is not effective.

Exclusions based on failure to complete a course of treatment.

Restrictions based on geographic location, facility type, provider specialty, and other criteria that limit the scope or duration of benefits for services provided under the plan or coverage.

It is important to note that the NQTL provisions referred to above are not prohibited outright; but are prohibited if they are applied more stringently to mental health / substance use disorder benefits than to medical surgical benefits.

Plans must apply comparable financial requirements (such as copay, coinsurance, deductible) for mental health / substance use disorder and medical surgical care.

The number of outpatient visits or inpatient days covered must be comparable for mental health / substance use disorder and medical surgical care.

Prior Authorization requirements for mental health / substance use disorder services must be comparable to or less restrictive than those for medical surgical services.

These standards are applied according to classifications of benefits:

- Inpatient / in-network
- Inpatient / out-of-network
- Outpatient / in-network
- Outpatient / out-of-network
- Emergency care
- Prescription drugs

MHPAEA Exceptions

Group health plans and health insurance issuers that are exempt from MHPAEA based on their increased cost (except as noted below). Plans and issuers that make changes to comply with MHPAEA and incur an increased cost of at least two percent in the first year that MHPAEA applies to the plan or coverage or at least one percent in any subsequent plan year may claim an exemption from MHPAEA based on their increased cost.

Large, self-funded non-Federal governmental employers that opt-out of the requirements of MHPAEA. Non-Federal governmental employers that provide self-funded group health plan coverage to their employees

(coverage that is not provided through an insurer) may elect to exempt their plan (opt-out) from the requirements of MHPAEA by following the Procedures &
Requirements for HIPAA Exemption Election posted on the Self-Funded Non-Federal
Governmental Plans webpage and issuing a notice of opt-out to enrollees at the time of enrollment and on an annual basis. The employer must also file the opt-out notification with CMS.

Medicare, Medicaid, and the Children's Health Insurance Program (CHIP) are not group health plans or issuers of health insurance. They are public health plans through which individuals obtain health coverage. However, provisions of the Social Security Act that govern CHIP plans, Medicaid benchmark benefit plans, and managed care plans that contract with State Medicaid programs to provide services require compliance with certain requirements of MHPAEA.

State vs. Federal

If a state has a stronger state parity law, then health insurance plans regulated in that state must follow those laws. For example, if state law requires plans to cover mental health conditions, then they must do so, even though federal parity makes inclusion of any mental health benefits optional. Federal parity replaces state law only in cases where the state law "prevents the application" of federal parity requirements. For example, if a state law requires some coverage for mental health conditions, then the federal requirement of equal coverage will overrule the "weaker" state law. NOTE: HHS has jurisdiction over public sector and DoL and the DoT have jurisdiction over private health plans.

If a plan must follow federal parity law, then the following must be covered equally when it comes to treatment limits and payment amounts:

- Inpatient in and out of network
- Outpatient in and out of network
- Intensive outpatient services
- Partial hospitalization
- Residential treatment
- Emergency care
- Prescription drugs
- Co-pays
- Deductibles
- Maximum out-of-pockets limits
- Geographic location
- Facility type
- Provider reimbursement rates
- Clinical criteria used to approve or deny care

Contact Us: Any team member who wishes to file a concern or complaint can contact us:

- New York Medicaid: 1-800-498-1453
- New York for all else: 1-800-333-8451
- Delaware Medicaid: 1-844-325-6256 • Delaware for all else: 1-438-2478

- West Virginia for all: 1-800-788-5301
- Pennsylvania Medicaid: 1-800-718-6400
- Pennsylvania for all else: 1-800-438-2478

Sources and References for more information are included to review the MHPAEA requirements / provisions.

References

Link to Mental Health Parity Bill: https://www.congress.gov/bill/104th-congress/housebill/4058/text

CMS Information / FAQs:

- https://www.cms.gov/CCIIO/Programs-and-Initiatives/Other-InsuranceProtections/mhpaea_factsheet
- https://www.cms.gov/cciio/resources/fact-sheets-and-faqs#Mental%20Health%20Parity Medicaid Sources

Delaware	https://regulations.delaware.gov/register/august2017/general/21%20DE%20Reg%20158%2008-01-17.htm
New York	https://omh.ny.gov/omhweb/bho/docs/nys-mhpaea-report.pdf
Pennsylvania	https://www.insurance.pa.gov/Coverage/Pages/Mental-Health-ParityFAQs.aspx
West Virginia	https://www.wvlegislature.gov/wvcode/ChapterEntire.cfm?chap=33&art=16&section=3FF#:~:text=Mental%20health%20parity.&text=Includes%20autism%20spectrum%20disorder%3A%20Provided,all%20utilization%20review%20as%20applicable
	https://dhhr.wv.gov/BBH/DocumentSearch/Get%20Connected/Advocacy%20Resources/Mental%20Health%20Parity.pdf

Privacy Act of 1974

The Privacy Act of 1974 is a United States federal law, establishes a Code of Fair Information Practice that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies.

Social Security Act (SSA)

Medicare is a national social insurance program administered by the U.S. federal government and falls under the Social Security Act, or SSA. As such, Highmark Health is required to follow all statutes, policies, rules, and associated amendments related to Medicare Parts A-D.

The Stark Statute also falls under the SSA. This law prohibits a physician from making referrals for certain designated health services to an entity when the physician or a member of his/her family has an ownership/investment interest or has a compensation arrangement.

CIVIL MONETARY PENALTIES FOR VIOLATIONS OF THE SOCIAL SECURITY ACT

The Office of Inspector General (OIG) may impose civil penalties for several reasons, including:

- Arranging for services or items from an excluded individual or entity.
- Providing services or items while excluded.
- Failing to grant OIG timely access to records.
- Knowing of and failing to report and return an overpayment.
- Making false claims.
- Paying to influence referrals.

Damages and Penalties: The penalties can be around $15,000 to $70,000 depending on the specific violation. Violators are also subject to three times the amount:

- Claimed for each service or item or
- Of remuneration offered, paid, solicited, or received.

Example*:* A California pharmacy and its owner agreed to pay over $1.3 million to settle allegations they submitted unsubstantiated claims to Medicare Part D for brand name prescription drugs the pharmacy could not have dispensed based on inventory records.

Gifts and Entertainment Policy

As a reminder, there are laws around gifts and entertainment we can accept and/or provide. Highmark Health's policy regarding gifts or entertainment is that both may be offered or accepted in connection with customers, business partners, vendors, suppliers, or other individuals and entities that do or seek to do business with Highmark Health, provided the value of the gift is a small, non-cash item.

As a general rule, workforce members may only accept or give gifts that are unsolicited, infrequent, not in violation of the Code of Business Conduct, may not create a conflict of interest, and does not compromise or appear to compromise the workforce member's ability to make objective decisions that are in the best interest of the company.

Workforce members should never offer or accept gifts from government officials or government employees. For detailed information related to gifts and business courtesies, workforce members should refer to the Gifts and Entertainment Policy or Code of Business Conduct.

When in doubt, contact your people leader or a representative from Enterprise Risk and Governance.

Combatting Fraud, Waste, and Abuse

It's important to understand that there are differences among healthcare fraud, waste, and abuse. One of the primary differences is intent and knowledge.

Healthcare Fraud occurs when someone knowingly and willfully obtains or attempts to obtain money or property owned by any health care benefit program through actions that they know are wrong.

Healthcare Waste occurs as the result of over-utilization of services or other practices that result in unnecessary costs to the health care system. Healthcare waste does not involve monetary gain but is the result of inappropriate or inefficient use of resources including supplies, time, or unnecessary spending.

Healthcare Abuse includes actions that may, directly or indirectly, result in unnecessary costs to the company and/or federal or state government. Abuse involves receiving payment for items or services when payment is not required and where the provider has not knowingly misrepresented facts to receive payment.

Types of Fraud, Waste, and Abuse

The four types of fraud, waste, and abuse that are common in our industry include Healthcare Fraud, Financial Reporting Fraud, Corruption, and Prescription Drug Fraud.

Healthcare Fraud includes provider and health insurance fraud where a person or group of people knowingly obtain money or property under false pretenses from a health care benefit program.

Financial Reporting Fraud is the false reporting of financial information to mislead those relying on the financial statements. This type of fraud often occurs when senior leaders or management intentionally manipulate financial information to meet certain expectations, such as a year-end bonus.

Corruption is dishonest or illegal behavior, performed by people who lack integrity. In business, it is the inappropriate use of influence on a business transaction to obtain individual benefit, or benefit for someone else. Engaging in bribery, receiving kickbacks, or receiving side payments are forms of corruption.

Prescription (Rx) Drug Fraud includes knowingly distributing or obtaining prescription drugs under false pretenses, or knowingly double billing for a medication. Rx waste often happens when providers switch medicines during treatment, leaving medicines unused. Waste also occurs when patients are prescribed inappropriate or unnecessary medications. And Rx Abuse occurs as the result of the over-prescribing of medications such as opioids or other controlled substances.

Who Makes a Difference?

The one thing that fraud, waste, and abuse has in common is you. Our workforce members are our biggest resource when it comes to combating these issues. The most common method of fraud detection is the anonymous employee tip.

This is just one more way to raise the bar and elevate Highmark Health's Compliance program.

You may be wondering how you can spot a fraudster. Well, according to KPMG's "Profiles of a Fraudster", the people who commit fraud are typically experienced employees in a position colluding with others inside and outside of their organization. Fraudsters usually hold managerial or senior executive positions and do not have a prior history of criminal activity. The fraudster tends to be highly respected and appears trustworthy. 85% of fraudsters are first time offenders and are not part of an organized criminal element.

Fraudsters could be your coworker, your neighbor, or even a health care provider.

Note that KPMG is a global network of professional firms providing Audit, Tax and Advisory services.

What would you do?

You are reviewing recent expense statements for a coworker that seem out of the ordinary. The expense statements are for activities that occur during non-working hours and are for excessive amounts. You recall

that this coworker has been complaining about their finances as well as voicing disagreement with company policies in public settings.

Given the number of red flags you are seeing, you decide to report the coworkers expense statements to which department?

Enterprise Risk and Governance
Technical Assistance Center (TAC)
Corporate Communications

Feedback: Report possible fraud to Enterprise Risk and Governance through the Integrity Hotline at 1-800-985-1056.

How Can You Stop Fraud, Waste, and Abuse?

Since our workforce members are our best and most valuable tool to prevent fraud, waste, and abuse, it is important to know how to prevent, detect, and report these issues. We also want you to know how Highmark Health responds to fraud, waste, and abuse through corrective action and our internal auditing and monitoring programs.

You can prevent fraud, waste and abuse by leading by example and conducting yourself in an ethical manner.

Some examples of how you can prevent fraud include:

- Provide and maintain accurate data when requested and ensure timely billing.
- Understand fraud, waste, and abuse policies, procedures, standards, regulations, and CMS guidance.
- Verify information before taking action.

Attempt to detect fraud, waste, and abuse by identifying situations that could indicate wrongdoing.

Report unethical behavior, non-compliance, fraud, waste, or abuse to your leader or to Highmark Health Enterprise Risk and Governance.

Audit and monitor for fraud waste and abuse in your daily work. Once fraud, waste, and abuse are detected, Highmark Health is committed to preventing future occurrences by implementing education, auditing, and monitoring programs that prevent recurrence while maintaining compliance with any governmental requirements and ensuring that our customers are protected.

Potential Fraud, Waste, and Abuse Indicators

Now that you know how Highmark Health handles fraud, waste, and abuse, review the list of potential indicators or “red flags” that may be associated with these activities:

- Behavioral Indicators: Sometimes people behave in ways that could be indicative of their role in fraudulent activity. These behavioral indicators are by no means applicable to all situations and should be considered along with other information prior to assuming guilt or making a good faith report.

- Customer Red Flags: Fraud is also committed outside of Highmark Health by customers, or people pretending to be customers, to defraud a Highmark Health company or one of our partners, including Medicare or Medicaid.
- Claim forms and enrollment forms are one of the most common places where fraud can be detected. If processing or submitting claim forms or processing enrollment forms is a part of your job at Highmark Health, consider whether you have ever seen any of these potential indicators of fraud come across your desk.
- Credential fraud occurs when people posing as providers attempt to receive payment for services or attempt to enter practice without the proper education, training, or credentials. You can spot credential fraud by noting and following up on invalid license numbers, invalid name changes, and on situations where the name does not match the license number.
- Providers, workforce members of a provider, or employees of a provider may also be guilty of engaging in fraud. Additionally, provider fraud may be occurring if the provider or the patient is pressuring Highmark Health for rapid claim settlement or if identical treatment for all patients is found on claim forms. Provider fraud includes pharmacies.
- Insurance fraud refers to any duplicitous act performed with the intent to obtain an improper payment from an insurer.
- Manufacturer and wholesaler fraud can also attribute to monetary losses for the Highmark Health family of companies.

United Concordia Dental

For workforce members who are employees of United Concordia Dental, please review this section. For all other workforce members, skip to the Protecting Our Information section.

What is dental fraud?

Dental fraud is a specific kind of fraud that applies to our United Concordia workforce. Awareness of common dental fraud schemes will help improve this type of fraud detection and prevention.

There are different types of dental fraud that you need to be aware of as a member of the UCD workforce. Remember, fraud not only costs UCD money, but it also impacts you as a consumer of dental insurance and dental services. Fraud drives up your premium costs and your service costs.

Review each different types of dental fraud shown below to refresh your memory and note the types of fraud that apply in your work environment.

Types of Dental Fraud

- Balance Billing happens when a network dentist bills a patient for fees in excess of his or her deductible and/or applicable cost share for the treatment rendered.
- Doctor Shopping arises when a patient 'bounces' from one dentist to another for the purpose of obtaining prescriptions for controlled substances. The patient may be addicted to the drugs or may be selling the drugs for profit.

- Enrollment Fraud is when an individual or entity enrolls a person as a dependent or employee for the purpose of obtaining dental benefits.
- Free Services fraud is occurring when a dentist bills the insurance company for treatment rendered to a patient that was advertised as “free”.
- Identity Theft occurs when an imposter uses the personal identifying information of another to obtain dental benefits.
- Misrepresentation exists when an individual intentionally provides false, inaccurate, or misleading information that results in an unjust and/or fraudulent gain or reimbursement.
- Unbundling is when a dentist reports the integral parts of a procedure as separate procedures with the intent of obtaining a higher reimbursement.
- Up-coding exists when an individual reports a more expensive procedure than was actually rendered, with the intent of obtaining a higher reimbursement.
- Unlicensed Provider fraud occurs when an unlicensed individual treats a patient and then bills the cost of the treatment under the name of a licensed dentist.
- Unnecessary Treatment happens when a dentist performs a procedure that is not medically indicated or is not in accordance with the standards of dental care.
- Un-rendered Services occurs when an individual submits a claim for procedures that were not rendered to obtain reimbursement.

Identifying Dental Fraud

To combat dental fraud, United Concordia established the Special Investigations Unit, or SIU. This department is dedicated to investigating suspected fraud in all lines of United Concordia business. In order for fraud to be investigated by the SIU, it has to be detected by UCD employees.

Review the questions and match the situation to the type of dental fraud.

Situation 1

A dentist provides three (3) sealants to a patient but reports four (4) sealants on the claim form.

Unrendered Services Balance Billing

Feedback: This is an example of an Un-rendered Service. This type of fraud occurs when an individual submits a claim for procedures that were not rendered to obtain reimbursement.

Situation 2

A dentist provides a full-mouth series of x-rays, but instead of reporting the corresponding procedure code for a full-mouth series, the dentist reports the x-rays as eight individual films.

Unbundling
Up-coding

Feedback: This is an example of Unbundling. This type of fraud occurs when an individual reports integral parts of a procedure as separate procedures with the intent of obtaining a higher reimbursement.

Situation 3

A patient visits seven different dentists in a two-month period. Each dentist reports an emergency exam or palliative treatment but does not provide any definitive treatment to the patient. What type of dental fraud is being committed?

Enrollment Fraud
Doctor Shopping

Feedback: This is an example of Doctor Shopping. This type of fraud occurs when a patient goes from dentist to dentist for the purpose of obtaining prescriptions for controlled substances like drugs because of an addiction or with the intent to sell them.

Reporting Dental Fraud

If you suspect or detect dental fraud, report it to United Concordia Special Investigation Unit (SIU) by any of the following methods:

- Email: ucci.fraud@ucci.com.
- Using the online confidential complaint form:
  - www.ucci.com (commercial lines of business). ○ www.addp-ucci.com (ADDP only).
  - www.uccitdp.com (TDP only).
- Toll-free confidential fraud hotline 1-877-968-7455.
- Through U.S. or interoffice mail (SIU, 1800 Center Street, Suite 2B 220, Camp Hill PA 17011)

The SIU conducts thorough investigations of all fraud allegations and evaluates all evidence collected during the investigation to determine the appropriate course of action. Actions may include:

- Education
- Overpayment recoupment
- Focused review (flags)
- Referral to local, state, or federal agencies
- Network termination

The SIU welcomes any referral of suspected fraud. However, there are some commonly misdirected referrals:

1. Quality issues are handled by Contract Compliance for the TRICARE Dental Program and Active-Duty Dental Program only, or Grievance for all other lines of business.
2. Routine Billing. Routine billing issues are handled by Customer Service.
3. Forgery. Customer Service will issue an affidavit to the complainant if there are concerns about forgery.

Resources

- PolicyWeb: http://policyweb.synergy.local/ ○ Enterprise Fraud, Waste, and Abuse Policy ○ Enterprise Gifts & Entertainment Policy

- Highmark Health Integrity and Compliance site: https://highmarkhealth.sharepoint.com/sites/IntegrityCompliance/SitePages/Combating.as px

Protecting Our Information

No one wants their private and personal information out there in the open. Anyone who has had their information end up in the wrong hands, or those who have been a victim of a cyber breach or identity theft, understand how distressing it can be.

You know that you can't release information pertaining to AHN patients or Highmark members to your family or friends. But did you know that anything you create, write, design, or develop for our company while using company property becomes property of Highmark Health? And, as a result, those work products must be kept confidential?

Did you know that you can't take pictures and video in the workplace? This includes anywhere in your home where you have your work laptop. That also means those fun videos or memes must be created outside of work, and not in the hospital or in the office.

Keeping things private and protecting our company's confidential information is a big step towards security and safety. You need to actively think about securing confidential information. We are fighting every day against cyber criminals, and they are always thinking of new ways to infiltrate our defenses, steal confidential information, and to use it to their advantage.

It's been said that there are only two types of companies: those that have been hacked, and those that will be.

That is why this section of the course is so vitally important. We need to be vigilant every day to stop cybercrime from taking place at our company. After all, it's not just our patient's and member's private information that's on the line, it's your confidential information too.

This section of the course is broken down into these topics:

- Confidential Information
- Contractually Sensitive Information
- New York State Requirements
- Competitively Sensitive Information
- Information Use, Management, and Disclosure
- Physical Workplace Safeguards
- Cyber Security

Take the time to review each module in this section so that you are empowered with the tools you need to help protect our information.

Confidential Information

Introduction

Confidential Information is all information either generated by Highmark Health – or made available to Highmark Health – for the purposes of conducting its business operations. This is the type of information we will focus on in this section of the course.

Confidential Information can exist in electronic format, on paper, and even in conversation. Examples include:

- Paper: contracts, financial reports, patient charts, lab results, etc.
- Electronic: information in enrollment & claims systems, emails, chats, and text messages.
- Conversation: business meetings, negotiations, etc.

We prefer not to share Confidential Information outside the company, but if we need to, we do so in accordance with Highmark Health policies and procedures.

Types of Confidential Information

At Highmark Health, we differentiate between several different types of Confidential Information. Review a brief description of each type of Confidential Information you may encounter at Highmark Health.

Consumer Data

Consumer Data is any information that identifies, describes, relates to, or can reasonably be linked to a consumer as defined by any state, federal, or international consumer privacy law.

For example, California has a comprehensive privacy law commonly referred to as "CCPA". This law regulates the way we can collect, use, and disclose information about California consumers. Some examples of consumer data are things like: customer purchasing history or patterns, Geolocation data and biometric information such as a fingerprint.

Competitively Sensitive Information

Competitively Sensitive Information, or CSI is nonpublic information held by Highmark Health, Highmark, Inc., and Allegheny Health Network including past, present and future reimbursement rates and rate schedules; contracts with providers; contracts with payers; terms or conditions of payer/provider contracts that could be used to gain an unfair commercial advantage over a competitor or supplier including discounts, reimbursement methodologies, pay for performance, pay for value, tiering of providers, cost data and methodologies including specific cost and member information and revenue, discharge information specific to payer or provider; contract negotiations including offers, party positions, thought processes; specific plans regarding future negotiations or dealings with payers or providers, and claims reimbursement data.

We'll learn more about CSI in another portion of the training.

Financial Information

Financial Information is non-public information maintained in the usual course of business by Highmark Health's finance area including budgets, investment documents, and credit card information.

Group Customer Information

Information that relates to our group customers, who are the companies who purchase their employee health coverage from us. This type of information includes contract terms and conditions, enrollment information for members who are covered by a certain group, and claims data.

Human Resources Information

Information maintained by the Human Resources Department, or which is otherwise related to members of the Highmark Health workforce. May include compensation, performance evaluations, employee benefits, and employee leave information.

Personally Identifiable Information (PII)

Personally Identifiable Information (PII) is any information about an individual that can be used on its own or in combination with other information to identify, distinguish or trace an individual's identity.

Proprietary Information

Proprietary information is information in which Highmark Health has an ownership interest.

Everything created during the course of your work is owned by Highmark Health and is considered proprietary and confidential. This includes PowerPoint presentations, strategic plans and corporate strategy, authorized research or academic papers, and spreadsheets.

Protected Health Information

Protected Health Information or PHI is identifiable information about an individual that relates to an individual's past, present, or future medical condition, receipt of health care, or payment for health care. PHI also includes any patient photographs or medical imaging.

PHI may only be accessed, used or disclosed in the following situations:

1. For treatment, payment, or health care operations.
2. As permitted or required by a particular law or corporate policy.
3. According to the terms of a contract.
4. With the appropriate authorization.
5. In accordance with the Highmark and AHN Notice of Privacy Practices.

Protected Health Information in Depth

PHI may not be shared or used unless its purpose is allowed under HIPAA. One set of permitted purposes is commonly known as TPO.

Treatment requires the sharing of information between providers so that the patient can receive the care they need. An example of this would be when a specialist sends correspondence to a patient's primary care physician to update them on a plan of care.

Payment involves any exchange of information that helps to pay claims or provide coverage and benefits to our members and patients. An example of this would be when a physician sends clinical documentation to a patient's insurance company to obtain prior authorization for a prescribed medication.

Health Care Operations are activities such as an exchange of information for our daily business operations. This could include quality assessment and improvement activities, audits, fraud and abuse detection and prevention, business planning and development and the training of employees.

Note that if your use of PHI does not fall under one of these categories, then you MUST obtain authorization from the individual to share his or her information.

Provider Information

Provider Information is any non-public provider-specific data including proprietary fee schedules, productivity targets, and contractual obligations.

Contractually Sensitive Information

Contractually confidential information includes any sensitive information that Highmark Health or its affiliates is in possession of as a result of a contractual agreement with an external third party.

Let's look at what this means for Highmark.

Highmark Health and enGen have access to certain payer information, including competitor rates, as a result of the work performed by enGen for its customers.

This information is not only competitively sensitive but is also contractually confidential and may not be used for any purpose other than in the course of providing contractually agreed to services for the customer providing the confidential information.

In particular, this information may not be used as part of our strategy to enter or serve the southeastern Pennsylvania market.

What would you do?

A workforce member of Highmark Inc. is negotiating rates with providers in southeastern Pennsylvania. The Highmark Inc. workforce member believes that his colleague who works at enGen has access to competitor rates in this region that could help in pricing Highmark Inc.'s rates.

Can the Highmark Inc. workforce member ask his colleague at enGen for these competitor rates?

Yes
No

Feedback: No, the workforce member cannot ask his colleague for these rates. This information is competitively sensitive and contractually confidential. The information may not be used in Highmark Inc.'s market entry into southeastern Pennsylvania. Workforce members at enGen shall only use this information in the course of providing services to its customers.

New York State Record Requirements

Due to the integrated nature of our business, it's important to keep in mind that the state of New York has specific rules related to Human Immunodeficiency Virus (HIV)-Related Information and Mental Health Records. These rules apply to patients and members who reside in the state of New York.

HIV-Related Information

Let's begin with how the New York State HIV Confidentiality Law impacts you, starting with how the law governs several activities including:

- HIV testing,
- Confidentiality,
- Reporting, and
- Partner notification.

The law safeguards Protected Individuals who:

- Have had an HIV test, whether positive or negative.
- Have an HIV infection, HIV-related illness/condition, or AIDS.
- Have been/are being tested for HIV or take medication specific HIV disease.
- Are a contact and/or partner of someone with HIV.

HIV Confidentiality Law

The New York State HIV Confidentiality Law requires:

An approved NYS standard HIV release form, completed in writing (oral authorization is not permitted) and signed by the individual or his/her personal representative to disclose information.

You must maintain the confidentiality of any HIV-related information you receive during the performance of your job - and even after you leave your job here - whether or not the person has had no contact with the plan.

HIV Disclosures

Disclosures of HIV-Related information are permitted without a properly executed HIV release form in these instances:

- To the individual or his/her personal representative, such as a parent or legal guardian.
- To an executor or an administrator of an estate to fulfill his/her administrative duties.
- Internal communications between medical professionals in the patient's treatment.

Mental Health Records

Now let's look at the New York State Clinical Records Confidentiality Law and the confidentiality of mental health records.

1. The New York State Clinical Records Confidentiality Law protects the confidentiality of mental health records. Specifically, the law prohibits facilities that provide services for the mentally disabled from disclosing any identifying information to any person or agency outside of the facilities.
2. Disclosure of mental health records is only permitted with proper patient authorization.
3. Disclosures of mental health records permitted without patient authorization include, but may not be limited to disclosures to:
    - Patient protection and advocacy services.
    - A parent of a child under 18 or an individual with a court-appointed legal guardianship.
    - The responsible division of the Federal Bureau of Investigation, for the purposes of responding to queries to the national instant criminal background check system, regarding attempts to purchase or otherwise take possession of firearms, in accordance with applicable federal laws and regulations.

Authorization for Release of PHI

When disclosing information in accordance with the law, utilize the New York State Required Authorization for Release of Confidential HIV-Related Information or Authorization for Release of Confidential Protected Health Information (PHI) form for Alcohol and Substance Use Disorder Records and Mental Health Records.

Competitively Sensitive Information

Competitively Sensitive Information or CSI is a special type of confidential information that has its own policy. This policy governs how competitively sensitive information can be shared within the Highmark Health family of companies.

The CSI policy describes the firewalls that separate and restrict the sharing of CSI between Highmark Health's provider and payer entities. The policy covers how CSI is shared between AHN, who is the provider, and the Health Plan, who is the payer.

CSI Firewalls

All employees should be familiar with these firewalls:

- Highmark Health personnel who have access to CSI belonging to Allegheny Health Network may not disclose it to Highmark Inc.
- Highmark Health personnel who have access to CSI belonging to Highmark Inc. may not disclose it to Allegheny Health Network.
- Allegheny Health Network personnel may not disclose Allegheny Health Network CSI to Highmark Inc.
- Highmark Inc. personnel may not disclose Highmark Inc. CSI to Allegheny Health Network.

See the Protecting Competitively Sensitive Information policy in PolicyWeb for more details. Note that PolicyWeb can be found in the Digital Hub.

Enterprise Data Governance

The Enterprise Data Governance Office or EDGO supports the organization by ensuring data assets are managed appropriately. Enterprise Data and Governance functions include overseeing shared data, identifying data owners and stewards, influencing data-related policies and procedures, helps inform data quality metrics, and creating metadata resources.

As a rule, any data that you plan to send outside the company, or to a different division within Highmark Health, should go through an Enterprise Data Governance Office, or EDGO, review.

Find out more about sharing information across the enterprise or outside the company by visiting the Enterprise Data Governance Office site.

Information Use, Management, and Disclosure

This module will focus on the Information Use, Management, and Disclosure policy which provides guidance and specific data-sharing policies and processes for each type of Confidential information.

Before sharing confidential information, you must determine if your actions could violate this policy based upon the type of data, who will use the information, and who will receive the information.

Minimum Necessary Rule

Anytime you are working with, or have access to Confidential Information, you need to remember the Minimum Necessary Rule, and consider how much information you need for a business purpose.
Ask yourself: “what, why, and who?” These questions will help you identify establish the framework for the minimum amount of information necessary to satisfy the request.

- What: Identify the minimum amount of information needed to satisfy the business purpose.
- Why: Identify and verify that there is a legitimate business need for the information provided.
- Who: Identify and verify who is associated with the needed information and to whom the information will be released, and that you’re only providing the information to someone who has a legitimate business need-to-know to do their job.

Exceptions to the Minimum Necessary Rule

Before we look at the guidelines for information sharing, review the exceptions to the minimum necessary rule.

The minimum necessary rule does not apply when:

- PHI is disclosed to, or requested by, a health care provider for treatment services.
- PHI is disclosed to a patient, member, or their personal representative.
- PHI is disclosed for uses or disclosures that are required by law.
- PHI is disclosed to the U.S. Department of Health and Human Services for compliance reviews or investigations.

Guidelines for Information Sharing

To help ensure you share or disclose information correctly, Highmark Health has established guidelines for information sharing. Review each of the guidelines listed below:

Authentication

Verify that you are sharing information with the right person. Follow the company guidelines to authenticate information. For example, selecting the wrong patient in Epic – or overriding a date of birth or Social Security number – can have serious patient safety and privacy consequences.

See AHN's Patient Identification Policy or the Highmark Knowledge Management Library Guidelines for additional details.

Accessing Your Own Information

The only information you are permitted to access is the information provided through your Workday account. You are never permitted to access your information, or ask a coworker to access your information, via systems such as INSINQ, EPIC or any other business-related platform.

Photography and Recorded Communication

Recording of "internal meetings" such as conversations with direct reports or "team huddles" is prohibited. Certain categories of meetings may be recorded including:

- Senior leadership recordings,
- Internal promotional produced video or audio communications,
- External promotional recordings, and
- Training and education.

Approval to record must be obtained prior to production of a recorded communication.

News Media Relations

Officers and workforce members of the Highmark Health family of companies who receive a request from the news media to speak on behalf of Highmark Health for business information or for an interview must refer the request immediately to the Senior Vice President of Corporate Communications or his/her staff member responsible for the media relations function.

Voicemail and Text Messages

Only leave confidential information in a voice mail message if authorized by the customer or patient. You are never permitted to send text messages that contain confidential information to anyone whether using a company or personal device.

The exceptions to this policy are communication with the patient and communicating Clinical Orders.

Here is the AHN-specific information about voice and text messages:

- Unsecure text messaging between providers, clinicians, and staff containing patient protected health information (PHI) is also prohibited. Review the AHN Text Messaging policy for additional guidance and information.
- The exceptions to this policy are communication with the patient and communicating clinical orders.
- If a patient requests to communicate with their providers directly via unsecured text messaging, you must obtain a written acknowledgement.
- You cannot use the standard text messaging app on your phone to communicate Confidential Information, even if you are using an AHN corporate device in the absence of the written acknowledgement.
- Placing clinical orders via text message is strictly prohibited. Confidential Information must be sent through AHN secure applications, such as EPIC Secure Chat which is accessible via Hyperspace, Haiku, Canto, Rover, PerfectServe or Voalte where available.

Epic Rules

Workforce members that have access to the Epic electronic medical records system must be careful to ensure protected health information or PHI remains confidential and avoid in unintentional sharing. Follow these general rules to ensure patient privacy:

- Use demographic information to verify that the correct patient has been selected.
- Verify provider name, specialty, and location before sharing PHI; verification avoids delays in patient care and misdirection of PHI.
- Recognize that Patient Confidentiality Forms are not a replacement for HIPAA Authorization
- Prior to scanning hardcopy information to a patient record, verify all patient identifiers match the patient record. When a hardcopy document is scanned into a wrong patient record, it may lead to inappropriate disclosure of PHI via MyChart. In addition, when scanning hardcopy information to a patient record, redact all full social security numbers and driver's license numbers on all pages prior to scanning.

For additional information, review the AHN Patient Identification Policy, the Mailing or Distributing Hardcopy PHI, and the Scanning Documents into the Medical Record policies found on PolicyWeb.

AHN EPIC-specific Rules

Use demographic information to verify that the correct patient has been selected.

If you are registering a patient at the time of service, always compare the patient with the photo ID on file, and have the patient confirm the demographics listed here to ensure you're working in the correct medical record.

- Complete Date of Birth.
- Complete Phone Number.
- Last Four (4) Digits of SSN if the phone number is unavailable or the Complete Address on File.

If you're verifying a patient over the phone, the patient must provide at least three of these identifiers. Don't read the patient's information to them, have them tell you! If these patient verification procedures aren't

properly followed, you are putting patient safety and privacy at risk. See AHN's Patient Identification Policy for additional details.

Prior to scanning hardcopy information to a patient record, verify all patient identifiers match the patient record. When a hardcopy document is scanned into a wrong patient record, it may lead to inappropriate disclosure of PHI via MyChart. In addition, when scanning hardcopy information to a patient record, redact all full social security numbers and driver's license numbers on all pages prior to scanning.

Be careful when entering Referring or Ordering Providers in a patient's electronic medical record. When selecting a provider-especially providers with similar names-confirm other identifier such as specialty, provider type, or office location. Don't simply select the first provider's name you see!

Selecting an incorrect provider during registration, or during order entry, will result misdirected PHI and could also delay the patient's care.

Let's take a couple moments to talk about when you can share information within Epic and with whom.

- Prior to sharing or discussing information with anyone other than the patient or the patient's treatment team, seek permission from the patient directly, or refer to the AHN Patient Confidentiality Form in the patient's medical record under the Media tab. If there's a Patient Confidentiality Form on file; the patient has given us permission to disclose limited PHI to a family member, caregiver, or friend.
- Pay close attention to special handwritten instructions or restriction requests on this Form: if you're unable to read the patient's handwriting or if the instructions are unclear reach out to the patient directly for clarification before disclosing information to anyone.
- This Form is effective until revoked by the patient; however, it should be updated by the patient annually as a best practice.
- This Form does not replace a HIPAA Authorization and does not give the named individuals permission to receive detailed health information contained within the medical record.
- Also, if a patient has listed you on their Form, that does not mean you can access that patient's information in Epic, or any other system.
- The Patient Confidentiality Form is valid only in the outpatient setting. For guidance on family communications in the inpatient, observation, or surgery center settings, refer to the Family Communication Policy, or your facility's PIN procedure.

Always remember to check the FYI Flag area in Epic to identify any restrictions that may be on the patient's record. Release Restriction flags indicate that additional steps must be taken prior to disclosing PHI, such as redaction of certain types of information as required by state or federal laws. Take the extra moment to ensure there are no restrictions on the patient's record before you discuss or disclose that patient's information.

Quick Disclosure: If a patient asks you for a copy of a recent lab result or office visit note from their Epic record, you need to document that patient's request in his or her Epic record. The Quick Disclosure function in Epic allows you to perform that documentation. Required fields include:

- To whom you're releasing the information.
- The date of the release.

- And what specifically was given to that individual.

If you have any questions about whether you should release something directly to a patient, reach out to Integrated Risk Operations for guidance. Remember you must check the FYI Flag field to ensure there are no release restrictions on that patient's record. MyChart is a way that patients communicate with our providers. With MyChart, patients can:

- Securely message their providers,
- Schedule appointments and video visits,
- Keep track of After Visit Summaries,
- Pay medical bills online,
- View test results, and
- Request prescription refills.

If a patient wants to designate someone else to use MyChart on their behalf, the MyChart Proxy process must be completed online. A patient's designee must have their own MyChart username and password and is not permitted to use the patient's MyChart account directly. If help is needed with the proxy process, you can refer them to the Frequently Asked Questions area on the MyChart homepage or reach out to the MyChart support team for guidance.

Visit mychart.ahn.org for more information, or to sign up for an account of your own.

For additional information, review the AHN Patient Identification Policy, the Mailing or Distributing Hardcopy PHI, and the Scanning Documents into the Medical Record policies found on PolicyWeb.

Social Media

The social media policy defines who is authorized to use company social media websites for business-related communications, and what information can be used.

You could be in violation of the social media policy if you:

- Post a member or patient's PHI to any social media platform.
- Use PHI to reach out to a member or patient via social media.
- Make reference to a member or patient's condition on your personal social media page. Doing so could violate both enterprise policies and HIPAA.

Simply omitting a name from your social media post does not mean you are protecting that individual's privacy. Other publicly available information or facts that could be obtained through an Internet search or press coverage could easily identify that person. Any workforce member who notices postings on social media that appear to include Confidential Information must promptly report the postings to the Highmark Health Integrated Risk Operations department using the email addresses shown.

Information Gatekeeper Policy

The Information Gatekeeper policy helps to monitor employees conduct with respect to Confidential Information throughout the various stages of the employment lifecycle.

This is another way that we protect Confidential Information.

The Gatekeeper process must be initiated when an employee plans to leave the organization to protect against the unauthorized transfer of Confidential Information.

See the information gatekeeper policy and training module within myLearning for more information.

Summary

Remember the minimum necessary rule: Disclosure of confidential information must be limited to the minimum amount of information necessary to satisfy a particular permitted purpose.

Always follow the information sharing guidelines found in the Information Use, Management, and Disclosure policy to ensure information is shared appropriately.

Physical Workplace Safeguards

As the way we work continues to evolve, we need to be mindful of physical workplace safeguards. This is another way we manage information. Physical safeguards are the methods we employ to keep our laptops, phones, paper-based information, and our business conversations safe.

Review the information for the work situation that best represents your most common work location by selecting the hyperlink below to go directly to that content:

- Remote work,
- On-site at a Highmark Health office, or
- In the clinical setting.

Remote Workplace Safeguards

When you are working remotely, the same rules apply as though you are in the office. There are six areas in your remote work environment that you should be careful to protect against unauthorized access.

Laptop

When you are working remotely, the same rules apply as though you are in the office. Your off-site work area should mirror your on-site work environment as much as possible and must be located in a private area that is not accessible to family, friends, or others without a business need-to-know. Family members and friends are not permitted to use your company-provided corporate devices for any reason. Lock your computer when not at your remote workstation.

You must use company-provided system access methods on a corporate device.

Personal Phone Use

If you have permission to use your personal mobile device for business, you must use companyapproved mobile software.

Webcam

Be mindful of your surroundings when on a video call. Use a background filter or erase any confidential information written on a whiteboard that is in view of the camera.

Documents

As with in the office, protect documents that contain confidential information by locking them in a desk drawer or filing cabinet when not in use.

Travel

If you are planning a trip outside of the United States, you must gain permission to take your company-issued device. Contact the Technical Assistance Center for approval or for a loaner device.

Shredding Documents

If you are finished with a hardcopy document that contains confidential information, you must shred those documents using a company-provided shredder.

Personal Virtual Assistant

Be mindful when working near personal virtual assistants. Parts of your conversation can be captured, even if you don't intend for that to happen, so it's important to disconnect these devices while working, or work in an area that is sufficiently distanced from them so that business conversations aren't picked up.

What would you do?

Lori took her corporate laptop home on Friday afternoon to catch up on some work over the weekend. She put her laptop in a bag and placed it on the back seat of her car. Once she got home and had dinner, she realized she forgot to bring in her bag. She parked her car on the street in front of her house - since the doors were locked, she figured she'd leave it there until the morning. The following day, Lori discovered that her car window was shattered: her bag and the laptop were missing. Lori reported the break-in to the local police.

What should Lori have done differently? Select the best answer.

She should have locked the laptop in her trunk.
She couldn't have prevented this: her car was locked, and her laptop was hidden in her bag.
She should have brought the laptop into her house with her when she got home.

Feedback

Lori's car was not parked in a secure location. She should have taken the laptop with her into the house.

On-site Workplace Safeguards

There are many areas in your Highmark Health workspace that you should be careful to protect. Review the safeguards needed to protect unauthorized access to confidential information.

Laptops and Computing Devices

Laptops or other computing devices must be cable locked or locked in a cabinet when not in use. Use only company-approved access methods and virtual collaboration software.

Document Disposal

NEVER use trash bins to dispose of documents or removable media that contain confidential information. Contact the Technical Assistance Center for information on disposal of flash drives or other removable media.

Document Storage

Secure all confidential information at the end of the day in a locked desk drawer or file cabinet. Do not leave any files, documents or binders that may contain confidential information on your desk.

Shredding Documents

When you no longer need hardcopy Confidential Information, place the documents in a designated locked shred bin in your area, or shred them yourself using a company-provided shredder.

Secure any boxes or other holding bins that may be used to temporarily store hardcopy documents to be shredded at a later time.

Taking Documents Offsite

Do not remove paper copies of confidential information from company premises unless you have a business need to do so, and you have your manager's approval.

Whiteboards and Task Boards:

Collect and secure any hardcopy information before you leave. Erase any notes made on a whiteboard or in collaborative spaces.

Copiers

Pick up printed materials and faxes at regular intervals during the day or use the secure print option.

Prior to leaving for the day, check shared printers, copiers, and fax machines to ensure you have collected and secured all confidential information.

At Your Desk

Laptop

Lock your computer screen whenever you walk away from your computer by using Control + Alt + Delete + Enter or similar function.

Use only company-approved access methods and virtual collaboration software.

Keys

Keys that secure corporate devices, hardcopy confidential information, and shred bins must not be left in locations where they are accessible to others.

Desk Phone

Immediately report any actual or suspected loss, misuse, or theft of corporate devices or information to the Technical Assistance Center.

Cell Phones

If you have received permission to use your personal cell phone for business, you must use the company-approved mobile software. Be mindful of your tone and surroundings when holding work related conversations.

Papers, Notebooks, Sticky Notes

All documents that may contain confidential information must be turned face down or removed from plain view whenever you leave your desk for short periods of time.

Lock Drawers

Always lock documents in a drawer, cabinet, etc. when the desk is unattended for significant lengths of time, or you leave for the day.

Clinical Workplace Safeguards

Workforce members who work in the clinical setting have additional safeguards that must be in place to protect confidential information and ensure patient privacy. There are six areas in the clinical workspace that require additional diligence and safeguards.

Monitor/Screen Lock

Use the Epic secure lock function or Control + Alt + Delete + Enter if you are away from your workstation. Protect patient health information by using a privacy screen on your computer monitor, when available.

Patient Privacy

Patient privacy is very important. Always obtain the patient's permission before discussing their condition in the presence of others in the room: don't assume that family members or friends in the room are permitted to listen to discussions of sensitive information. Some disclosures may require written authorization before you can discuss patient health information with someone other than the patient. This includes anything related to HIV/AIDS, behavioral health, or drug and alcohol or substance abuse-related information.

Refer to your facility's Family Communication Policy - or PIN procedure - before releasing Confidential Information to the patient's family, friends, or caregivers in person or over the phone.

In a semi-private room, use reasonable safeguards prior to discussing PHI, such as pulling the curtain, lowering the volume of your speaking voice, or using a private consultation room, if available.

Patient Courtesy

Prior to entering a patient's room, knock on the door and announce yourself. Introduce any students, residents, clinicians, or other hospital staff that may be with you.

White Board Information

Whiteboard information should be limited to the provided template or the approved data elements outlined in the AHN policy.

Hardcopy PHI

Handle hardcopy protected health information carefully. Do not leave PHI unattended where it could potentially be visible to those without a business need-to-know.

If you mail or distribute hardcopy PHI to a patient, follow the Mailing or Distributing Protected Health Information procedure. This procedure ensures that patients receive hardcopy information intended only for them. Each hardcopy page containing PHI must be verified and initialed by whomever is mailing or giving the documents to the patient. Mishandling documents that contain patient information may result in inappropriate disclosures of PHI.

Protect Patient Information

Confidential patient information may be found on IV bags, prescriptions, or other medical devices. Use a black marker to obscure any patient information that may be found on IV bags or other medical equipment prior to disposal.

What would you do?

Aimee is a nurse who periodically needs to leave her workstation-on-wheels, which is located in the hallway between patient rooms. She is documenting in a patient record when a co-worker asks for her assistance with another patient. Since the other patient is only a few rooms away, Aimee is able to keep an eye on her workstation: she minimizes her screen and she steps away for a couple minutes, so that she can pick up with her documentation where she left off.

Did Aimee follow approved methods for securing her workstation?

Yes No

Feedback: You are expected to lock your computer screen whenever you walk away from your computer.

Cyber Security

Thank you for taking the time to carefully review the Cyber Security content of this training course.

Healthcare is one of the most highly targeted industries for cyberattacks because of the significant amount of PHI, PII and CSI contained within our systems. Our organization recently experienced a data security incident which affected approximately 300,000 Highmark members, and the incident initiated when an employee clicked on a malicious phishing email.

It is critical that all employees understand the various types of cyber threats facing our organization, know how to spot these threats and how to report them. A cyber-attack can begin with only one person and so it's up to each of us to stay vigilant.

Cyber Security Risks

You wouldn't believe how many different types of cyber security threats are out there. This section of the course will cover the different types of phishing that could catch you and other types of cyber threats that you should be prepared to report.

Let's review the cyber security threats we face.

- Phishing is the practice of sending text messages designed to trick a human victim into clicking on a malicious link.
- Vishing is the practice of making phone calls or leaving voice messages designed to trick a human victim into revealing personal information.
- A business email compromise is when a legitimate business email account is compromised or impersonated to trick the recipient into conducting an unauthorized transfer of funds.
- Smishing is the practice of sending text messages designed to trick a human victim into clicking on a malicious link.
- And finally, spear phishing is a type of phishing in which the attack is targeted toward a specific group or individual.

Now let's look at how you can protect against these threats in detail.

Phishing

Phishing is an email fraud method in which the attacker sends out an email that looks legitimate and attempts to trick you into revealing sensitive information. This is how attackers gain your information and access to Highmark Health's network and confidential information.

Don't take the bait! Highmark Health's phishing awareness and prevention program periodically sends messages to your inbox that imitate a real phishing attack. While we block over 90% of unwanted emails into our system, real attacks get through, as they do with any organization. These phishing awareness program exercises are designed to arm you with the tools and knowledge needed to recognize a real phishing attack.

If you "take the bait" on these phishing exercises, you will be required to take additional phishing training courses. If you continue to "get caught" by these phishing exercises multiple times within a 12-month period, disciplinary action may occur, up to and including termination.

An example of a well-disguised phishing email is shown here, but if you look closely, you can spot the warning signs. Review this email. See if you can spot the clues that would lead you to believe this is a phishing email and should be reported.

> From: Microsoft 365 <noreply@account-microsoft365.com>, Subject: [External] Review these messages, Warning: This email originated from an external source and could contain harmful links or attachments. Use extreme caution. Report this to phishing@highmark.com if you suspect this is a harmful email. Microsoft365 logo, Review These Messages, 1 message is being held for your to riview

as of May 1.2022, Review them within 3 days of the received date by going to the quarantine page in the Security & Compliance Center or your account will be deleted.

Red Flag Indicators

These are the red flag indicators that it might be a phishing attempt:

- A sense of urgency, curiosity or pressure. Phishing e-mails create a sense of urgency to trick you into taking an action such as providing information, clicking on a link or opening an attachment.
- Unfamiliar email address or email address that isn't exactly correct. Do you recognize the sender's email address? Attackers will use variations of legitimate e-mail addresses to trick you into responding.
- Emails from outside the organization. Any email from outside of our organization will have an 'External' or 'External-Verified Sender' tag in the subject line.
- Links and buttons. Attackers can hide a malicious URL within a hyperlink that appears legitimate. Before you click, always hover your mouse over the button and see where the link actually takes you.
- Misspelled words and incorrect grammar. Would an email that comes from Microsoft 365 actually have grammatical mistakes or odd formatting? These are indicators of a suspicious and potentially harmful email.

Spot the Phish

As you look at this email, think about the following:

- Do you recognize this sender?
- Were you expecting to receive this file?
- Do you know where this link leads?
- This phish impersonates Microsoft to establish legitimacy.

Phishing email example:

From Microsoft OneDrive <notification@office.com>, Subject: A User Shared 2 Files With You Via OneDrive, Message: Hello User, You have two (2) fites awaiting review on One Drive Cloud, Review awaiting file(s) below: Payment_advice.pdf, Invoice.pdf, Button: Review Awaiting File

Here is another example. Review the following:

- Do you recognize this sender?
- This phish impersonates Microsoft to establish legitimacy.
- Personalized to grab your attention.
- Is there an appeal to urgency?
- Do you know where this link leads?

Email From: security@microsoft.com, Subject: Undelivered Messages, Office logo, Your messages couldn't be delivered. Microsoft found Several Undelivered Messages. Dear Mary: ACTION REQUIRED. How To Fix It: Retype the recipient's address, then resend the message – if you are using Outlook, open this non delivery

report message and click Send Again. In Outlook on the web, select this message, and then click the “Send Again” link located just below the message preview. Button Send Again.

What can you do to avoid getting caught?

Avoid clicking on direct links in emails where possible. Go directly to the source (Amazon, your bank) and log in through your browser or mobile application.

Be skeptical of any unexpected invoice, request for payment, request for validation of personal information, or offers for deep discounts that seem too good to be true.

Confirm that an email appearing to be from someone you know is legitimate via another communication channel, such as a phone call or Teams message. Never reply directly to the email and don’t use the contact information provided in the email.

If you believe an email is suspicious, please report it immediately by using the Report Phishing button in Outlook or forward the email to the email shown on your screen. Don’t delete, report!

We are counting on YOU to help stop the cyber criminals.

Vishing

Phishing isn’t the only way attackers try to steal your information. Phone calls and text messages are another way attackers try to trick you!

Vishing is the fraudulent practice of making phone calls or leaving voice messages claiming to be from reputable companies in order to induce individuals to reveal personal information.

Smishing

Smishing is the fraudulent practice of sending text messages with malicious links claiming to be from reputable companies in order to induce individuals to open malicious links or attachments.

Here is an example of a smishing text:

> WARNING:(Criminal Investigation Division) I.R.S is filing lawsuit against you, for more information call on ±1 7038798780 on urgent basis, Otherwise your arrest warrant will be forwarded to your local police department and your property and bank accounts and social benifits will be frozen by government.

Be on the lookout for phone calls and text messages that seem suspicious. Report any suspicious activity by calling the Technical Assistance Center (TAC) at 412-888-4822 or 1-800-561-2802.

Targeted Attacks

As a result of the increasing awareness around typical phishing tactics, cyber adversaries are adjusting their approaches by narrowing the scope and tailoring their fraudulent messages with details to convince the email recipient of their authenticity and compel them to act. This more focused approach to phishing is commonly called “spear phishing”.

Cyber criminals can build robust profiles of their targets' professional and personal lives. These profiles often include comprehensive relationship maps connecting their targets to many other people, which helps them find a way to gain your trust and compromise your security.

When an attacker utilizes spear phishing methods to go after a large, high-profile target, such as csuite executives, it's known as "whaling". To cyber criminals, executives and senior leaders hold tremendous value. Their access to company resources and the level of authority and trust held in the organization means that employees in these roles may be the most effective path to the valuable data they want. Additionally, cyber criminals are not above leveraging the personal assets and reputation of our executives and senior leaders to achieve their goals.

Business Email Compromise

In recent years, business email compromise, or BEC, has become one of the most prevalent and financially damaging types on online crimes, resulting in billions of dollars in organizational losses worldwide.

In a BEC scam, the attacker poses as someone the recipient should trust—typically a colleague, boss or vendor. This type of scam is frequently carried out when a subject compromises legitimate business email accounts through social engineering or computer intrusion techniques, or through a variety of impersonation techniques, such as domain spoofing and lookalike domains. The attacker seeks to conduct unauthorized transfers of funds such as asking the recipient to make a wire transfer, divert payroll, change banking details for future payments and so on.

BEC attacks are difficult to detect because they don't always use malware or malicious URLs that can be analyzed with standard cyber defenses. Instead, BEC attacks rely instead on impersonation and other social engineering techniques to trick people interacting on the attacker's behalf. Because of their targeted nature and use of social engineering, investigating and remediating these attacks is difficult and time consuming.

Protect Yourself

So, what can be done? Follow these five rules to protect yourself from a targeted attack. These rules apply to more than senior leaders and executives and can help prevent anyone from falling victim to a phishing attack.

1. Review privacy settings for social media accounts. If criminals know where you go, what you like, and information about your family and friends, they can build a profile for things like spear phishing. They can also attempt to gain access to you via your family and friends.
2. Check your Wi-Fi security settings. Ensure your firewall is on and that you have strong passwords for your wireless access, even your guest account, if you have one available.
3. Make sure your smart devices are not always listening. Ensure any smart personal assistants are not in a mode of constant listening and gathering of information.
4. Ensure any removable media, such as USB sticks and CDs, are kept in locked and secured areas. This applies to both in the office and when at home or traveling. These devices can be an easy gateway into our systems.
5. Avoid public charging areas as these locations do not provide the security needed to prevent a cyber-attack.

Ransomware

Ransomware is a type of malicious software designed to harm or exploit a device or network. Some ways you can potentially let ransomware on your computer are by clicking on a malicious phishing link or enabling macros on an attachment that you were not expecting.

Ransomware usually involves paying the attacker to get back your lost data and information.

If you suspect your computer has been infected with ransomware it is important to follow these steps:

- Don't attempt to use your computer.
- Don't turn off your computer.

Report the security incident by calling the support desk:

- For Highmark and UCD workforce members: Notify the Technical Assistance Center (TAC) by calling 412-888-4822 or 1-800-561-2802.
- For AHN workforce members: Notify the IT Service Center by calling 412-330-4357.

You are prohibited from paying the ransomware, regardless of how you believe the ransomware entered your computer or how inexpensive it may seem.

Password Hygiene

It may seem like you need a password to do anything and everything in today's digital world. Each time you access a new system or use a new application, you are likely thinking that you can't possibly remember yet another password. That is why password hygiene is so important.

Password hygiene is the practice of ensuring passwords are unique, difficult to guess, and hard to crack to keep your passwords safe from cyber criminals. Follow these guidelines when creating passwords:

- Create a pass*phrase*, rather than a pass*word*.
    - Use a song lyric, book title, or quote – any string of a few words that will be easy for you to remember but difficult for someone else to guess.
    - Add uppercase and lowercase letters, numbers, and symbols that conform to Highmark Health Enterprise standards. ○ Example: LionsTigersBearsOhMy!105
- Avoid using passwords that include family names, street names, or pet names.
- Avoid sharing your password with anyone.

Where possible, use a password manager, and never forget your passwords again!

Multi-Factor Authentication

Multi-Factor Authentication or MFA, also known as Two-Step Verification (2FA), is an authentication method that requires the user to provide two or more factors to gain access to an application, online account, or a VPN. Rather than just asking for a username and password, MFA requires one or more additional verification factors, such as a code you receive via email, SMS, or some sort of mobile app, or using fingerprints or facial recognition. You can think of MFA as a second layer of protection, a way of confirming your identity, and it's recommended to enable MFA wherever possible.

Recently, cyber adversaries have figured out a way to get past MFA on our Microsoft Authenticator tool using a social engineering technique called MFA Fatigue. MFA Fatigue is when an attacker will flood a targeted victim's email, phone, or registered device with multiple prompts to approve an MFA request. The goal is that the targeted user becomes so overwhelmed that they accidentally click on the Approve button or accept the MFA request to stop the surge of notifications they are receiving.

If you are receiving multiple prompts to accept an MFA request, please call the Technical Assistance Center (TAC) or AHN IT Service Center right away.

Insider Threats

Everything may not always be as it seems. Review the situations outlined below and determine which ones could be an indication of an insider threat.

Interest in matters outside of the scope of his or her duties.
Signs of vulnerability or hostile behavior.
Sending Confidential Information to a personal e-mail account.
Working odd hours or remotely accessing the network at unusual times.
Unexpected wealth, unusual foreign travel, or unexpected absences. Unnecessarily copying material, especially Confidential Information.

Insider threats come from individuals that you may know or interact with daily. These are people with intimate knowledge of the Highmark Health family of companies. Any of the situations listed could be an indication of an insider threat. These threats could come from current and former employees or contract partners whose behavior could be a risk to the company. Their actions may involve fraud, theft of confidential information, or the sabotage of our computer systems.

Report any suspicious activity:

- For Highmark and UCD workforce members: Notify the Technical Assistance Center (TAC) by calling 412-888-4822 or 1-800-561-2802.
- For AHN workforce members: Notify the IT Service Center by calling 412-330-4357.

Cloud Security Threats

Follow these cloud security guidelines to protect information that is stored on the cloud.

- Do not store or share any type of Confidential Information in cloud drives like SharePoint 365 or Google Drive unless it is the designated area for that information as set forth by your department.
- Do not use personal cloud storage for any reason on work devices or to store/send work related information.
- Be aware of setting permissions and accepting requests for cloud storage areas such as Microsoft Teams groups.
- Do not post Confidential Information on cloud community tools like Yammer.

Protecting Our Information Resources

Links to departments, groups, and policies that were referred to in this section are listed below. A comprehensive list of resources is found in the Appendix. Visit PolicyWeb to access all Highmark Health and AHN policies listed below.

PolicyWeb: http://policyweb.synergy.local/

- Protecting Competitively Sensitive Information Policy
- Acceptable Use of Electronic Communication Policy
- Communications to News Media Policy
- Enterprise Social Media Policy
- Recorded Communications Policy
- Information Use, Management, and Disclosure Policy
- Scanning Documents into the Medical Record Policy
- AHN Patient Identification Policy
- AHN Mailing or Distributing Hardcopy PHI Procedure Policy
- AHN Text Messaging Policy

Data Ethics, Policy, and Privacy Department: https://highmarkhealth.sharepoint.com/sites/Privacy

Information Security and Risk Management: https://highmarkhealth.sharepoint.com/sites/InformationSecurity

Enterprise Data Governance Office: https://highmarkhealth.sharepoint.com/sites/EnterpriseDataGovernance

Enterprise Data Sharing Standard (STD 5085163): http://policyweb.synergy.local/Home/PolicyDetails/5085163

Highmark Knowledge Management Library Guidelines: https://highmrk.saas.verinthms.com/GTConnect/UnifiedAcceptor/FrameworkDesktop.Main

Contact Information

If you want to learn more about cyber security, have a question and don't know who to ask, or want to know your cyber risk score, visit us at **infosec.highmark.com**.

Visit PolicyWeb and search for the Acceptable Use of Electronic Communication and Information policy. After reviewing this important policy, bookmark it to return to if you have questions.

Seeking Advice and Reporting Concerns

There's a lot of information to digest and sometimes it can seem overwhelming. But remember that you are not expected to be compliance, privacy and security expert. You are expected, however, to do your best. Do the right thing and do your part to raise the bar for everyone we serve.

How do you do that? It's not so much about always having the right answer, it's about knowing where to go to find the right answer.

In this section, we are going to review the six aspects of seeking advice and reporting concerns.

Retaliation-free Workplace

Sometimes it is hard to stand up and report something that is wrong and involves a friend or a coworker.

Remember, that if you raise the bar and offer your best to others, then you deserve the same or better. Reporting violations will not result in retribution or retaliation by any Highmark Health company or members of the Highmark Health workforce.

Per our company policy, any individual found to have engaged in Retaliation or in acts of intimidation against another individual will be subject to corrective action, up to and including termination of employment.

Highmark Health Code of Conduct

The Highmark Health Code of Conduct acts as our guide for conducting our business with integrity and ensuring compliance. As a member of the Highmark Health team, you have a responsibility to report any potential or actual violation of the Code of Conduct or any suspected or known privacy incidents.

Good Faith Reporting

Good Faith Reporting is raising an issue or a concern in a timely manner with no ulterior motive. It is also raising an issue or a concern that could be a violation of our Code of Conduct, the law, regulations, or policy. Remember, no type of reporting in good faith can result in retribution or retaliation, so if you have a concern, you have an obligation as a Highmark Health workforce member to speak up and report your suspicions or observations.

What Happens Next?

All reports of suspected violations are reviewed and investigated by Highmark Health's Enterprise Risk and Governance Division and an appropriate response will be implemented, which may include further reporting to governmental agencies, including law enforcement.

And, while all reports are confidential, there are situations where information may be shared as required by law.

What would you do?

A coworker tells you that he looked up a football player's medical records and he knows whether the player is going to retire early or get back on the field this season!

Tell him you don't want to know and change the subject. It's going to get out anyways. Call your bookie!

Don't give him the chance to tell you. But you need to report what you heard, when you heard it, and who said it.

Feedback: That's right! Don't give him a chance to tell you. Suspected privacy incidents or known privacy violations must be reported immediately to Integrated Risk Operations at integratedriskandprivacyops@highmarkhealth.org.

Data Ethics, Policy, and Privacy

We all have a responsibility to ensure that we, as a company, exercise care, caution and due diligence when collecting and handling Confidential Information. The Data Ethics, Policy, and Privacy Handbook is your guide to Highmark Health's privacy and security policies.

When it comes to privacy incidents, keep in mind that you are responsible for reporting any suspected unauthorized activity, non-compliance, attacks, and intrusions so that we can continue to protect our customer's and our company's private information. Suspected privacy incidents or known privacy violations must be reported immediately to the Privacy Department. Time is of the essence!

- If you learn about a computer security or data breach or intrusion, it must be reported to the Information Security & Risk Management Department (ISOC) or to the Technology Assistance Center (TAC).
- AHN workforce members that suspect a computer security or data breach should call the IT Service Center.

How to report a computer security or privacy incident:

Computer Security or Data Breach

Computer security or data intrusions must be reported to the Information Security & Risk Management Department (ISOC):

- Highmark and UCD workforce members: isoc@highmark.com or 1-800-561-2802.
- AHN workforce members should call the IT Service Center at 1-412-330-HELP (4357).

Privacy Incident

Suspected privacy incidents or known privacy violations must be reported immediately to Integrated Risk Operations at r 1-866-228-9424 or at Integratedriskandprivacyops@highmarkhealth.org

All reports are considered confidential.

What would you do?

A nurse walked away from a computer at the nurses' station and forgot to lock it. When he returns, several new screens are open, and it looks like someone was searching patient records.

Should he report it?

Yes
No

Feedback: That's right! This should be reported immediately! AHN workforce members that suspect a computer security or data breach should call the IT Service Center at 412-330-HELP (4357).

Reporting Suspected Misconduct

Raise the bar to protect our customers and our business and report concerns about suspected misconduct, privacy concerns, or computer breaches.

Reach out to the Integrity and Compliance office for any of the following:

- Policy, Procedure, and Code of Conduct questions or violations.
- Compliance questions or concerns.
- Suspected or detected compliance violations.
- Fraud, Waste, or Abuse questions.
- Suspected or detected Fraud, Waste, or Abuse.

For Highmark Health and UCD workforce members, contact the Integrity and Compliance office anonymously through the Helpline toll-free at 1-800-985-1056. You can also email us at integrity@highmarkhealth.org.

For AHN workforce members, contact the Integrity and Compliance office anonymously through the Helpline toll-free at 1-877-867-7325. You can also email us at integrity@highmarkhealth.org.

Resources

Links to departments, groups, and policies that were referred to in this section are listed below. A comprehensive list of resources is found in the Appendix. Visit PolicyWeb to access all Highmark Health and AHN policies listed below.

PolicyWeb: http://policyweb.synergy.local/

- Search for the Non-Retaliation Policy.

Effective Lines of Communication site:
https://highmarkhealth.sharepoint.com/sites/IntegrityCompliance/SitePages/Initiatives.aspx

Highmark Health Code of Conduct:
https://www.highmarkhealth.org/hmk/pdf/highmarkHealthCodeBusinessConduct.pdf

Highmark Health Third Party Code of Conduct:
https://www.highmarkhealth.org/hmk/pdf/highmarkHealthThirdPartyCodeBusinessConduct.pdf

Conclusion

There are several resources for workforce members. Then complete the Attestation and Certification.

For those workforce members that need CME/CNE/CE Credits, instructions are included at the end.

Quick Reference Guide

Download the included quick reference guide (QRG) for a list of Highmark Health's confidential lines of communication. The QRG provides you with methods for anonymous and good-faith issue reporting if you suspect or detect unethical conduct, noncompliance, fraud, waste, or abuse.

Remember that all inquiries and reports are handled in a confidential manner, subject to limitations imposed by law.

CME/CNE/CE Credits

Continuing Medical Education, or CME, consists of educational activities which serve to maintain, develop, or increase the knowledge, skills, and professional performance and relationships that a physician uses to provide services for patients, the public, or the profession.

Download the Physician, Nurse, or Non-Physician Workforce Members PDFs for further instructions.

Appendix

For list of the resources and definitions throughout this course, download the Appendix.

Thank you for completing the 2023 Annual Compliance, Information Security, and Privacy course.

