AULTMAN

HIPAA & Compliance Education

2023 - 2024

Aria Walker

Chief Compliance and Privacy Officer

The **Aultman Compliance Program** was established to support our **commitment to the highest standards of conduct, honesty and integrity in our business** practices.

Compliance is all about **doing the right things for the right reasons all the time.**

Compliance programs exist to identify and oversee corrective actions. It's important that you understand that anyone can identify and report a compliance concern. When in doubt, ask! Talk with someone about your concerns, use the confidential compliance line or call us in the Compliance office. If you're concerned about something, then we're concerned about it, too.

Thank you for taking the time to complete this important education. Most of all, thank you for your continuous effort each day to protect the privacy of our patients and to perform your work with honesty and integrity.

AULTMAN

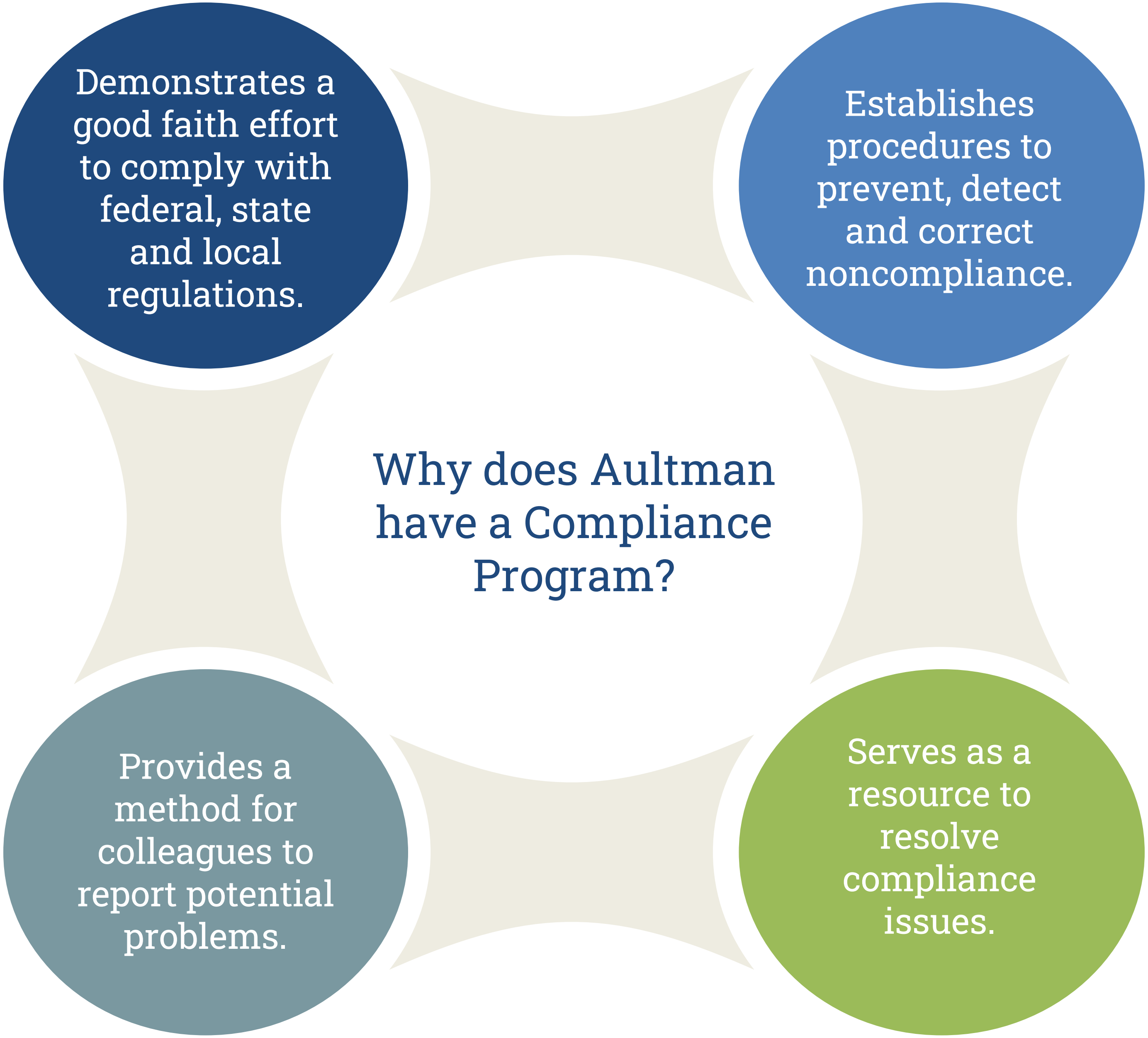
Topics:

- About Aultman's Compliance Program
- Aultman Code of Conduct
- Colleague Expectations
- Fraud, Waste & Abuse (FWA)
- Emergency Medical Treatment and Labor Act (EMTALA)
- How to Report a Compliance Concern

Healthcare Compliance

It's everyone's RESPONSIBILITY

AULTMAN



Why does Aultman have a Compliance Program?

Demonstrates a good faith effort to comply with federal, state and local regulations.

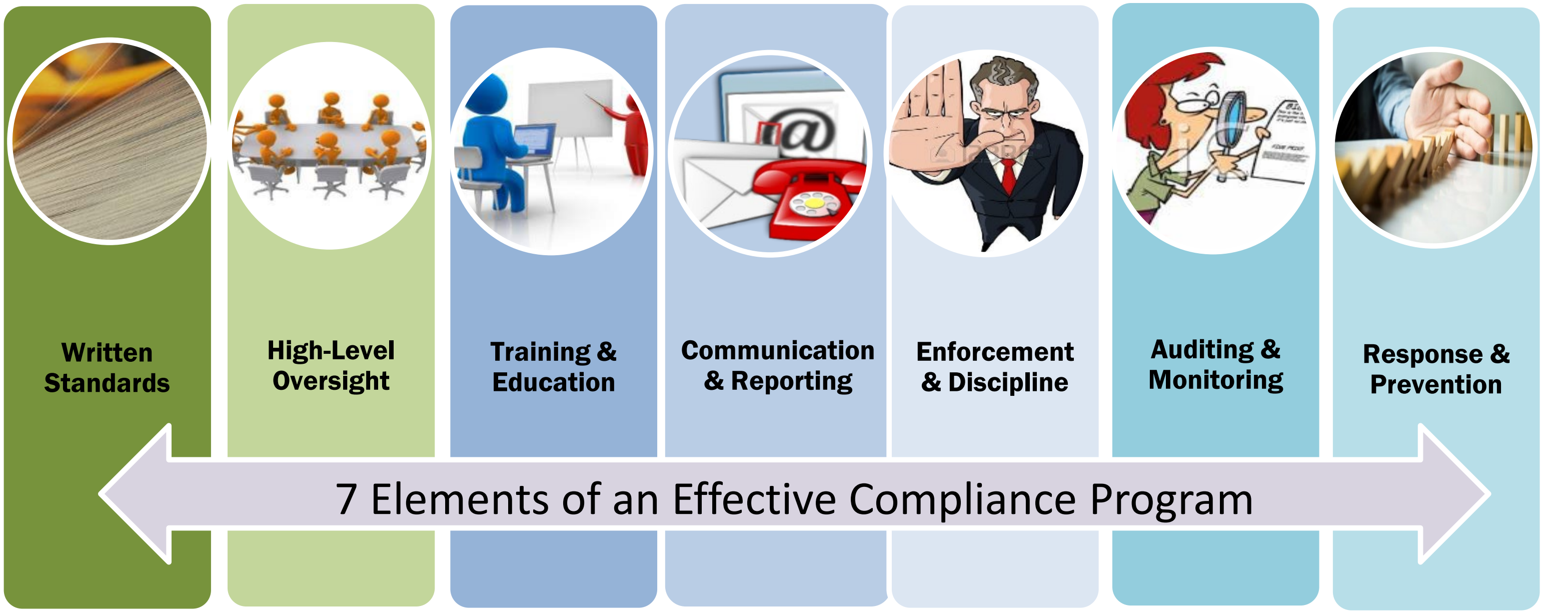
Establishes procedures to prevent, detect and correct noncompliance.

Provides a method for colleagues to report potential problems.

Serves as a resource to resolve compliance issues.

The Aultman Compliance Program

Aultman's Compliance Program is modeled after the Federal Office of the Inspector General's Compliance Guidance, which includes seven specific elements to prevent, detect and correct business conduct that does not conform to applicable laws and regulations.



Written Standards

High-Level Oversight

Training & Education

Communication & Reporting

Enforcement & Discipline

Auditing & Monitoring

Response & Prevention

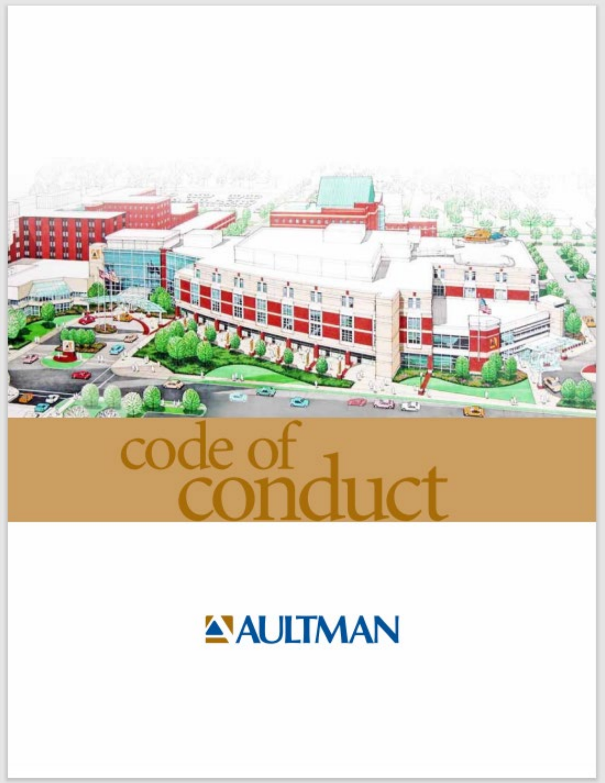
7 Elements of an Effective Compliance Program

Aultman Code of Conduct

The Aultman Code of Conduct is the foundation of the compliance program and defines Aultman's expectation and commitment to legal and ethical business practices for all colleagues.

Aultman's Corporate Code of Conduct:

- Transfers our values into general guiding principles;
- Provides guidance to help colleagues meet ethical and legal standards;
- Contains the key statements of acceptable business practices, conflicts of interest, and expected standards of ethical and moral behavior;
- Contains resources to help resolve any questions about appropriate conduct in the workplace; and
- Governs all of our relationships.



Expectations of an Aultman Colleague

Follow Aultman's Code of Conduct

Carry out your job duties with honesty and integrity

Know the laws and regulations that apply to your job

Exercise good judgment and do the right thing

Report suspected concerns and problems

Everyone is required to promptly report violations of actual or suspected noncompliance.

There can be NO retaliation against you for reporting in good faith.

Fraud, Waste & Abuse (FWA)

Government agencies, including the Department of Justice, the Department of Health & Human Services Office of Inspector General (OIG), and the Centers for Medicare & Medicaid Services (CMS), are charged with enforcing laws that combat Fraud, Waste & Abuse.

U.S. Department of Health and Human Services
Office of Inspector General

FRAUD

An intentional act of deception, misrepresentation or concealment in order to gain something of value.

WASTE

Over-utilization of services and/or the misuse of resources.

ABUSE

Excessive or improper use of services or actions that are inconsistent with acceptable business or medical practice.

Emergency Medical Treatment and Labor Act (EMTALA)

EMTALA was enacted by Congress in 1986 and was designed to prevent hospitals from transferring uninsured or Medicaid patients to public hospitals without, at a minimum, providing a medical screening examination to ensure they were stable for transfer.

This law **REQUIRES** Medicare-participating hospitals with dedicated emergency departments, like Aultman, to screen and treat the emergency medical conditions of patients in a non-discriminatory manner to anyone, regardless of their ability to pay, insurance status, national origin, race, creed or color.

- **Hospitals must keep a central log** to include information on each individual who comes to the hospital seeking treatment for a perceived emergency medical condition. The Central Log includes patients from other areas of the hospital that may be considered dedicated emergency departments such as Labor and Delivery.
- **A hospital must report to CMS or the state survey agency** any time it has reason to believe it may have received an individual who has been transferred in an unstable emergency medical condition from another hospital in violation of EMTALA.
- The Department of Health and Human Services (HHS) Office of the Inspector General (OIG) may impose a civil **monetary penalty on a hospital or provider for an EMTALA violation. CMS may also penalize a hospital by terminating its provider agreement.**

Hospitals have three main obligations under EMTALA:

1. **Any individual who comes to the emergency department for a perceived medical emergency must receive a medical screening examination by an authorized provider to determine whether an emergency medical condition exists.** Examination and treatment cannot be delayed to inquire about methods of payment or insurance coverage. Emergency departments also must post signs that notify patients and visitors of their rights to a medical screening exam and treatment. Signage that could deter patients from seeking emergency care could be an EMTALA violation.

2. **If an emergency medical condition exists, treatment must be provided until the emergency medical condition is resolved or stabilized.** If the hospital does not have the capability to treat the emergency condition, an "appropriate" transfer of the patient to another hospital must be done in accordance with the EMTALA provisions.

3. **Hospitals with specialized capabilities are obligated to accept transfers from hospitals who lack the capability to treat unstable emergency medical conditions.**

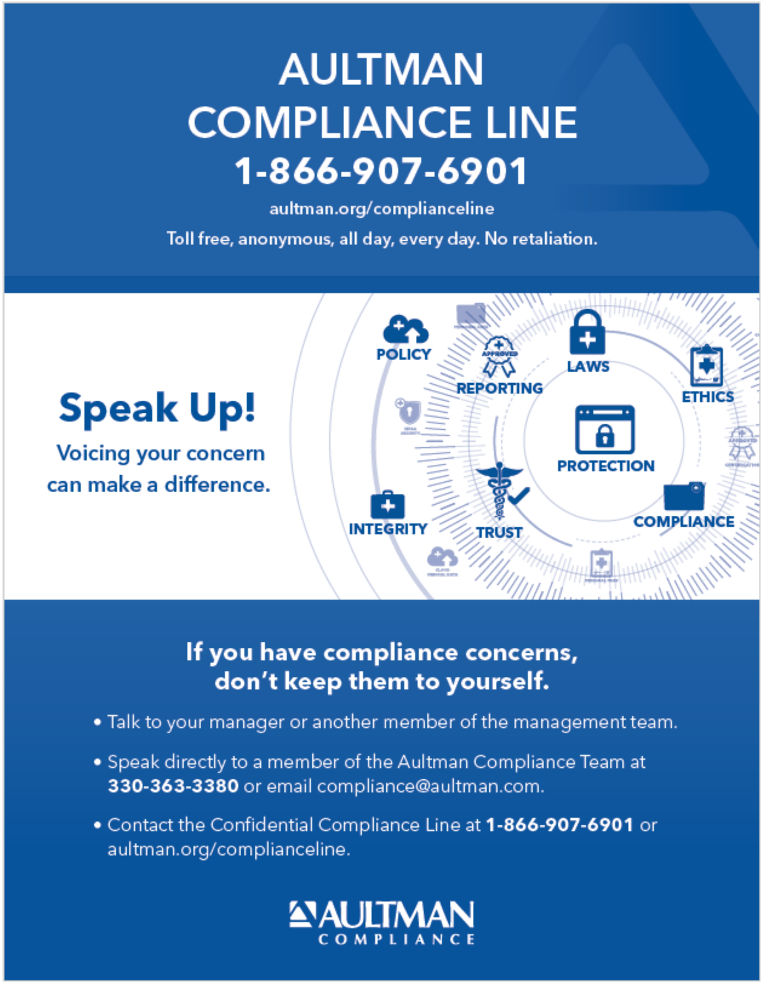
How to Report a Compliance Concern

- Discuss concerns with your manager or another member of the management team.

- Contact the **Compliance department** at:
  - 330-363-3380
  - Ext. 33380
  - compliance@aultman.com

- Report **anonymously** by calling the **Aultman Compliance Line** at:
  - 1-866-907-6901
  - Or online at https:www.aultman.org/complianceline

  (This hotline is managed by a third-party company and sends the anonymous report to the Compliance department for investigation and resolution.)



AULTMAN COMPLIANCE LINE

1-866-907-6901

aultman.org/complianceline

Toll free, anonymous, all day, every day. No retaliation.

Speak Up!

Voicing your concern can make a difference.

POLICY
REPORTING
LAWS
ETHICS
PROTECTION
INTEGRITY
TRUST
COMPLIANCE

If you have compliance concerns, don't keep them to yourself.

- Talk to your manager or another member of the management team.
- Speak directly to a member of the Aultman Compliance Team at **330-363-3380** or email compliance@aultman.com.
- Contact the Confidential Compliance Line at **1-866-907-6901** or aultman.org/complianceline.

AULTMAN COMPLIANCE

Employees reporting in good faith will not be subject to retaliation.

Topics:

- What is HIPAA?
- Who Must Comply with HIPAA?
- Protected Health Information (PHI)
- Minimum Necessary Standard
- Sharing Information with a Patient's Family & Friends
- Do Not Publish (DNP)
- Emergency Department Patient Information
- Snooping / Unauthorized Access to Patient Information
- HIPAA Audits
- Pay Attention to Detail

HIPAA Compliance

HIPAA compliance is adherence to the physical, administrative and technical safeguards outlined in the HIPAA Privacy Rule, which Aultman must uphold to protect the integrity of Protected Health Information (PHI).

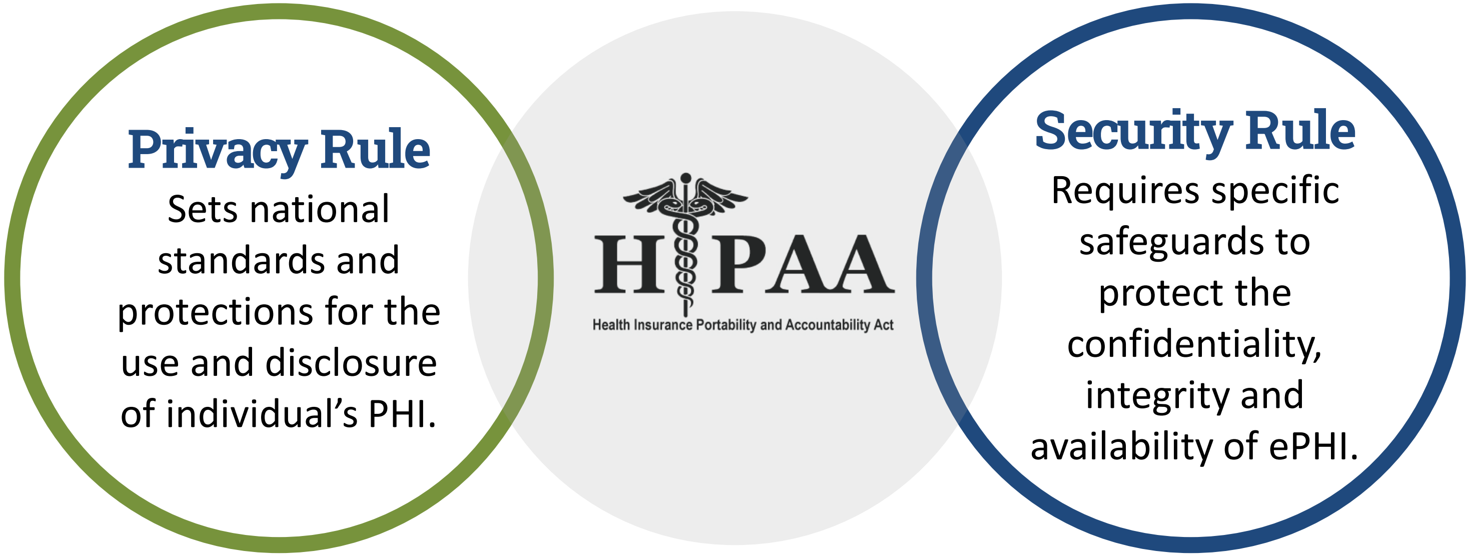
AULTMAN

What is HIPAA?

Health Insurance Portability and Accountability Act

The federal law establishing privacy and security standards to protect an individual's medical records and other health information provided to health plans, doctors, hospitals and other healthcare providers. Under these standards, Aultman is required to protect patient Protected Health Information (PHI) and Electronic Protected Health Information (ePHI).

HIPAA rules have two parts:



Privacy Rule

Sets national standards and protections for the use and disclosure of individual's PHI.

Security Rule

Requires specific safeguards to protect the confidentiality, integrity and availability of ePHI.

Who Must Comply with HIPAA?

- Those who must comply with HIPAA are often called HIPAA-covered entities. These include, but are not limited to:

  - Hospitals
  - Physician Practices
  - Clinics
  - Nursing homes
  - Rehab facilities
  - Pharmacies
  - Healthcare workers
  - Health insurance companies
  - Health maintenance organizations (HMO)
  - Employer-sponsored health plans
  - Government programs that pay for health care, such as Medicare, Medicaid, and military and veterans' health programs

- HIPAA does NOT apply to life insurers, employers, workers' compensation carriers, most schools, law enforcement, many state agencies like child protective services, reporters, restaurants or grocery stores.

Protected Health Information (PHI)

Any health information that could identify a person.

May include:

- Patient name, address, age, date of birth, social security number, clinical information, test results, diagnosis, photos, employer, etc.
- Can be in any form including electronic, paper or oral.

Some examples of PHI:

- ✓ Medical records
- ✓ X-rays
- ✓ Claims or billing records
- ✓ Conversations with patients
- ✓ Blood test results
- ✓ Health information regarding a person who has been deceased less than 50 years.

Examples of information that is *not* PHI:

- × Employment records held by an employer, like:
  - × Sick leave requests
  - × Drug screening as condition of employment
  - × Disability insurance forms
- × Family Education Rights and Privacy Act (FERPA) records
- × De-identified health information

HIPAA
Minimum Necessary Standard

This important HIPAA standard emphasizes that even when using Protected Health Information (PHI) for a job-related reason, you should only access, use or disclose the information that is **minimally necessary to complete the task you are trying to accomplish.**

- Looking at your own information or the information of a family member does NOT meet this standard!
- Minimum Necessary Standard does NOT apply to disclosures made:
  - For treatment purposes.
  - To an individual about his or her own PHI.

A billing clerk may need to know that a particular test was performed, but not the results of the test.

When making an appointment, a scheduler may need to look at when the previous appointment was, but not the patient's entire schedule history.

If a provider needs to know about a patient's family history, they should look in the patient's record but not the actual records of family members.

Sharing Information With a Patient's Family & Friends

Health information may be shared with designated family, friends or others who are involved in a patient's care or payment with the patient's approval.

- **Obtain patient approval before sharing PHI.**
  - Oral or written approval is acceptable.
  - Document it in the medical record.
  - The patient may change their mind at any time.
- **Use professional judgment when the patient cannot speak for themselves.**
  - Only disclose the minimum amount of information necessary.
  - Family & friends should be actively involved in care in order to receive PHI.

Do Not Publish (DNP)

- Patients choosing to opt out and be excluded from the Aultman patient directory are considered **Do Not Publish or a DNP patient**.
- Calls or inquires for a DNP patient should be answered: **"We have no information on anyone by that name."**
- When asked about the location of a patient, colleagues should contact the information desk or transfer the call to the hospital operator. They should NOT access the patient's record.

HIPAA allows Aultman to maintain a directory containing certain information about a patient that **CAN** be disclosed to the general public. This directory includes the patient's name, location and a one-word statement of condition.

Additional Information

- DNP does not apply to clinical staff who have a need to know.
- Clinical areas can share information with the patient's authorized family members/friends. No information should be shared with the general public.
- The patient may share their information on their own with anyone.

Emergency Department Patient Information

DO NOT access the Emergency Department Tracking Board unless you have a job-related reason to do so.

- Only those colleagues caring for the patients in the Emergency Department should be accessing and viewing the ED Tracking Board!
- Access to the ED Tracking Board is tracked with auditing software for inappropriate or unauthorized access.
- Remember – just because you are able to access a patient's record DOES NOT mean that you are authorized to view the information.

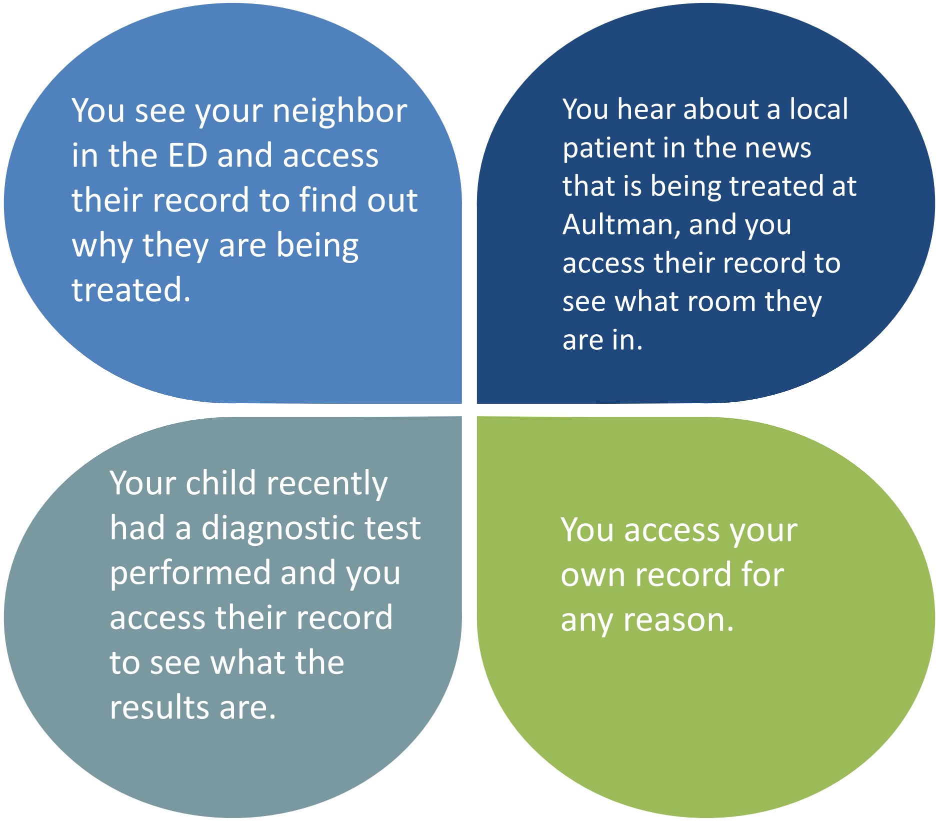
Snooping and Unauthorized Access

Snooping is when a colleague accesses the record of an individual for a reason that is not job-related, regardless of intent.

- Aultman polices **DO NOT PERMIT** colleagues to look up their own medical information, or that of family, friends, co-workers or patients of interest.

- Colleagues can appropriately access their medical information through the patient portal, *Aultman OneChart*.

Examples of snooping



You see your neighbor in the ED and access their record to find out why they are being treated.

You hear about a local patient in the news that is being treated at Aultman, and you access their record to see what room they are in.

Your child recently had a diagnostic test performed and you access their record to see what the results are.

You access your own record for any reason.

HIPAA Audits

Aultman is required to have audit trails of electronic medical record access and utilizes specialized software for this purpose.

An audit report can show **WHO** accessed a record, **WHEN** it was accessed, and **WHAT** information was viewed.

Colleagues may be asked to justify their access into a record, and any access deemed to be unauthorized may result in disciplinary action.

Remember… **YOU** are responsible for **ANY** access that occurs under your login password.

Pay Attention to Detail

We are all susceptible to errors. “Pay attention to detail” is an HRO tool designed to prevent us from making unintended slips and lapses when we perform familiar, routine acts as if we are on autopilot.

Using the **STAR** method for those critical points of no return allows us to minimize distractions and concentrate on the task at hand.

STOP – pause before you do anything.

THINK – about what you’re about to do.

ACT – when you actually perform the task.

REVIEW – check to make sure you’ve done exactly what you’ve meant to do.

Common examples of errors that could lead to HIPAA violations and potentially affect patient safety:

- ☒ A patient receives another patient’s discharge paperwork.
- ☒ Results are sent to the wrong provider due to the wrong information being chosen from a drop-down list.
- ☒ A fax being misdirected due to not entering the correct fax number.
- ☒ Scanning patient information into the wrong medical record.
- ☒ Individuals receiving the billing statement for another patient due to the wrong information being entered or selected.

Test your HIPAA Knowledge

Q: A colleague who does not work in the Emergency Department has some down time during their shift and is curious to see if there is anyone that they know in the ED, so they access the ED Tracking Board to take a peek. Is this ok?

A: NO. This is not permissible. The colleague does not have a job-related reason to do this.

Q: You had blood work done recently and as an Aultman colleague you know that you are not permitted to use your Aultman login password to access your own health information within the system. Instead, you ask a co-worker to access your results for you. Is this ok?

A: NO. This is not permissible. Your co-worker does not have a job-related reason to do this.

Q: You are out to lunch with your friend Sam who reveals that he is having surgery. He asks you not to tell anyone, but you let it slip to another mutual friend. Sam finds out that you told your other friend and is angry. He claims that because you are a healthcare worker you violated HIPAA. Is this true?

A: NO. You did not learn this health information while doing your job.

Q: You see a news report about a local car accident and the reporter says the patient has a broken leg as a result. Is this a HIPAA violation?

A: NO. Newspapers, TV stations and other media are not HIPAA-covered entities so their reporters cannot violate HIPAA. If a healthcare worker learned of that information while doing their job and disclosed it to the reporter without permission, the healthcare worker has violated HIPAA.

Q: An individual calls the Emergency Department and asks what room their mother has been admitted to. Is it ok for you to access the patient's record to look up the room number and tell the individual?

A: NO. When asked about the location of a patient, Colleagues should call the information desk. They should NOT access the patient's record.

Q: You work at a physician's office and access the AultPIN system to retrieve a new patient's information. While in there, you decide to look up your ex to see what lab work they have had drawn recently. Is accessing your ex's information ok?

A: NO. You do not have a job-related reason to do this. Just because you have access does not mean you are authorized to access/view all patient information.

Topics:

- Why Is Cybersecurity Important to Healthcare?
- Mobile Devices
- Social Media

Cybersecurity Awareness

Cyberattacks are one of the biggest threats facing health care systems today, and the best defense is prevention.

AULTMAN

Why Is Cybersecurity Important to Healthcare?

Healthcare organizations are particularly vulnerable and targeted by cyberattacks because they possess so much information of high monetary and intelligence value to cyber thieves and bad actors.

- Stolen health records may sell up to 10 times or more than stolen credit card numbers on the dark web.
- Patient safety and care delivery may also be jeopardized. Losing access to medical records and lifesaving medical devices, such as when a ransomware virus holds them hostage, may deter our ability to effectively care for patients.
- The targeted data may include patient’s PHI, financial information like credit card and bank numbers, SSN and intellectual property related to medical research and innovation.
- Hackers’ access to private patient data not only opens the door for them to steal information, but also to either intentionally or unintentionally alter the data, which could lead to serious effects on patient health and outcomes.

Mobile Devices

Mobile devices such as laptops, tablets, smartphones and USB flash drives that contain confidential Aultman information must be **password protected** and **encrypted**.

- Pictures of patients and items such as X-rays, patient lists or computer screens may not be taken with personal cell phones or devices.
- Texting of patient information should only be performed with Aultman approved platforms that are secure and encrypted.

The government prohibits the texting of patient care orders, regardless of the platform used.

Social Media

Never forget that the information you learn as part of your work at Aultman is confidential and should not be shared on social media. HIPAA requires this.

Even if just one person can identify the patient you are posting about, the post is identifiable.

What should you avoid?

- × Posting pictures of patients.
- × Complaining about patients or mentioning patients while complaining about your job.
- × Blowing off steam after a hard day, such as posting about a difficult experience with a very sick patient.
- × Commenting on news stories about patients who are being treated at Aultman.
- × Letting people know that a celebrity, politician or other prominent person is being treated at Aultman.
- × Adding information to threads other people have started.

Best practices

- ✓ Do not list Aultman in your employment section.
- ✓ Do not reference events that happen at work.
- ✓ Keep social media conversations with co-workers limited to personal, non-work events.
- ✓ Do not send pictures of patients to your friends – they may put them on social media.
- ✓ Do not add or follow any patients on social media that you met through work.

HIPAA regulations require Aultman to provide ongoing compliance education for all colleagues and other members of the Aultman workforce. We have created a post-test to demonstrate your understanding of the information provided in this education. Every colleague must complete the post-test and answer 80% of the questions correctly.

Please proceed to the post-test now.