AULTMAN

Compliance & HIPAA Education

2024 – 2025
Volunteer Team

Aria Walker

Chief Compliance and Privacy Officer

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.

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 support organizational adherence to legal and ethical standards, mitigate risks, enhance patient safety and to outline organizational responsibilities.

You are a key part of Aultman's compliance program. 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**.

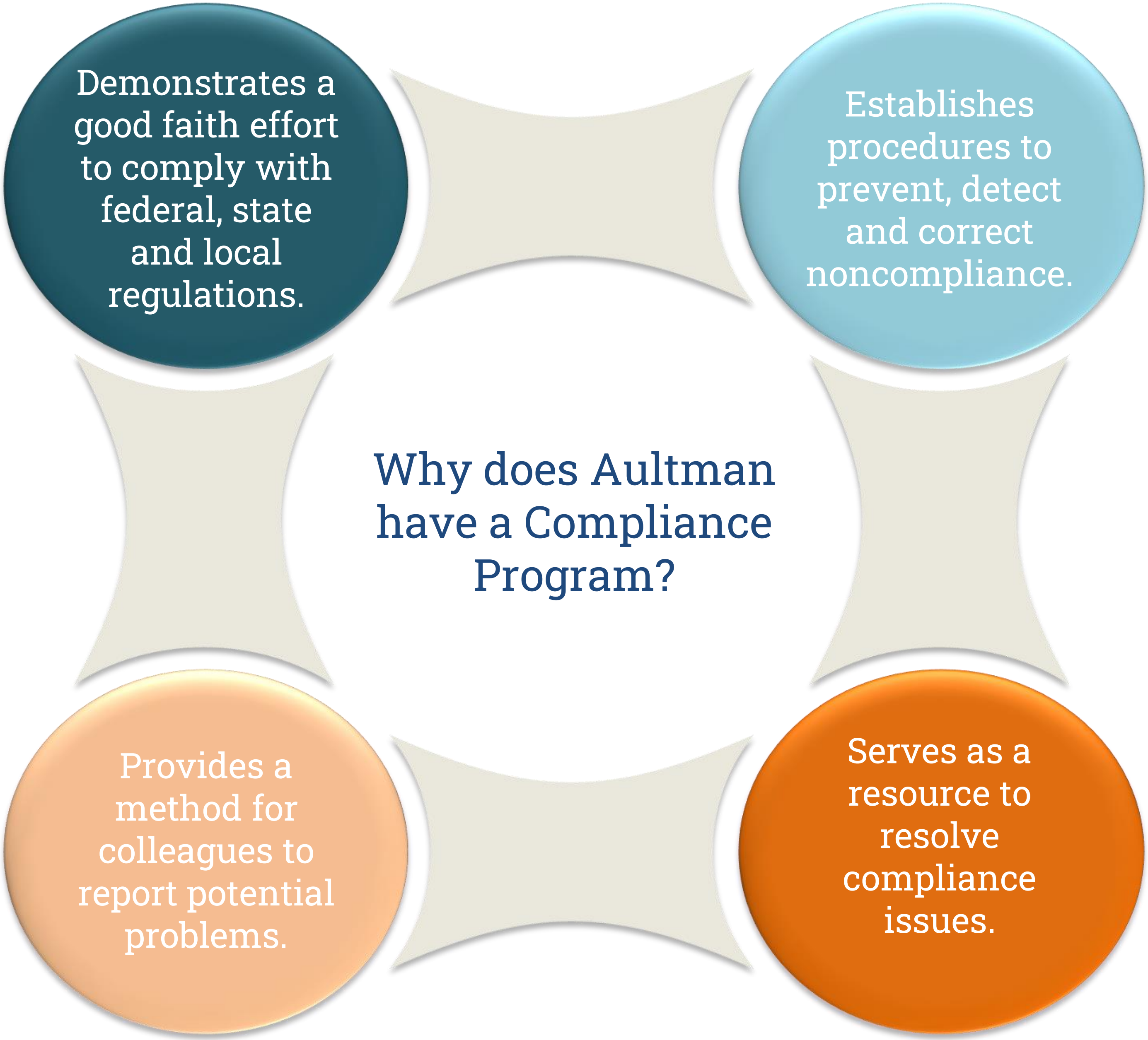
Topics:

- 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.

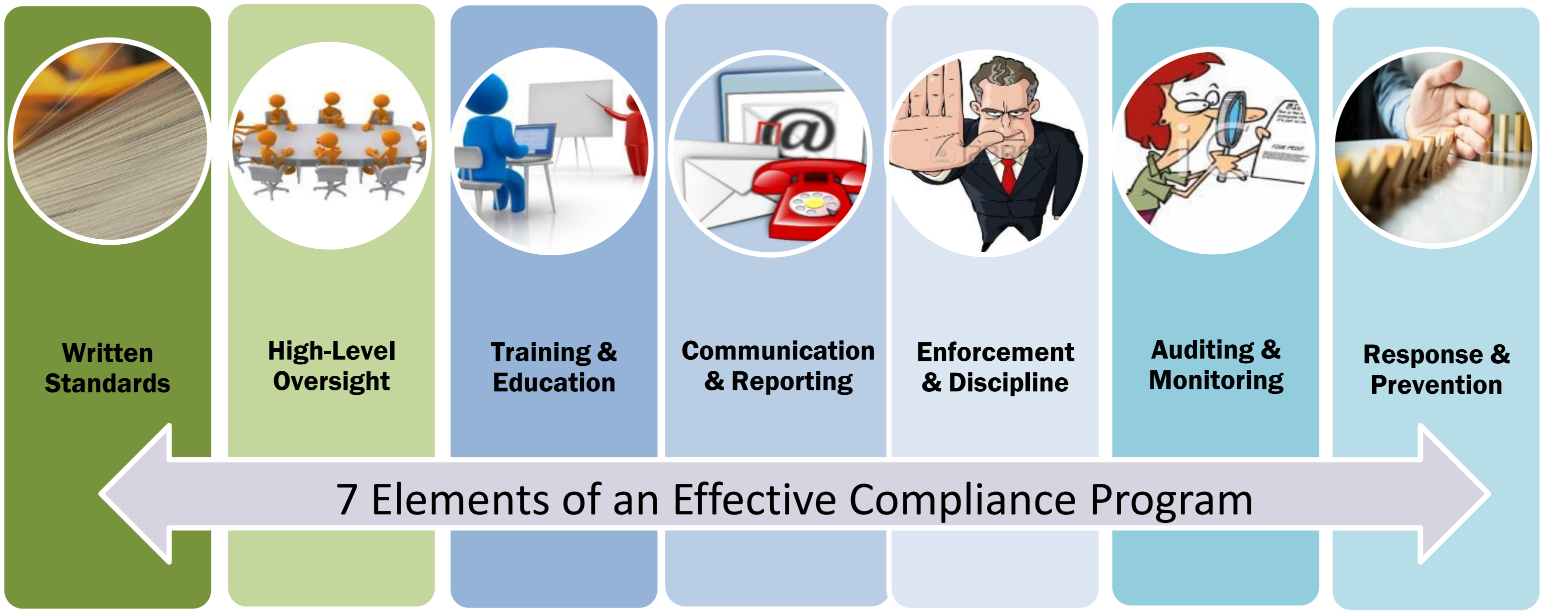
Establishes procedures to prevent, detect and correct noncompliance.

Serves as a resource to resolve compliance issues.

Provides a method for colleagues to report potential problems.

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.



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:

- Defines Aultman’s general guiding principles;
- Provides guidance to help colleagues meet ethical and legal standards;
- Outlines 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.

code of conduct

AULTMAN

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 is NO retaliation against you for reporting in good faith.

Fraud, Waste & Abuse (FWA)

Aultman's **Compliance Program** is also established to **prevent and detect fraud, waste, and abuse**. FWA is the intentional and unintentional actions that result in the misuses of resources, funds or services.

FWA violations can result in criminal and/or civil penalties.

FRAUD

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

- Example: Billing for services not provided.

WASTE

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

- Example: Unnecessary lab tests.

ABUSE

Practices inconsistent with sound fiscal, business or medical standards.

- Example: Requesting reimbursement for services that are not medically necessary.

U.S. Department of Health and Human Services

Office of Inspector General

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

Prevention of Fraud

To help prevent possible fraud, what should you do?

✓ Clearly and legibly document all information/procedures in the medical chart, including who requested and provided the service.

- If it is not documented, it cannot be billed.

✓ Be aware of problems that keep occurring, especially payment denials, as these can be signs of possible false claims.

✓ Do not do something just because “everyone else is doing it.” This does not make it right! If you have a concern about whether you are performing a task correctly, ask your supervisor.

✓ Be careful when starting new processes. Be sure the change does not cause incorrect claims to be submitted or other errors, which may result in fraud.

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.

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

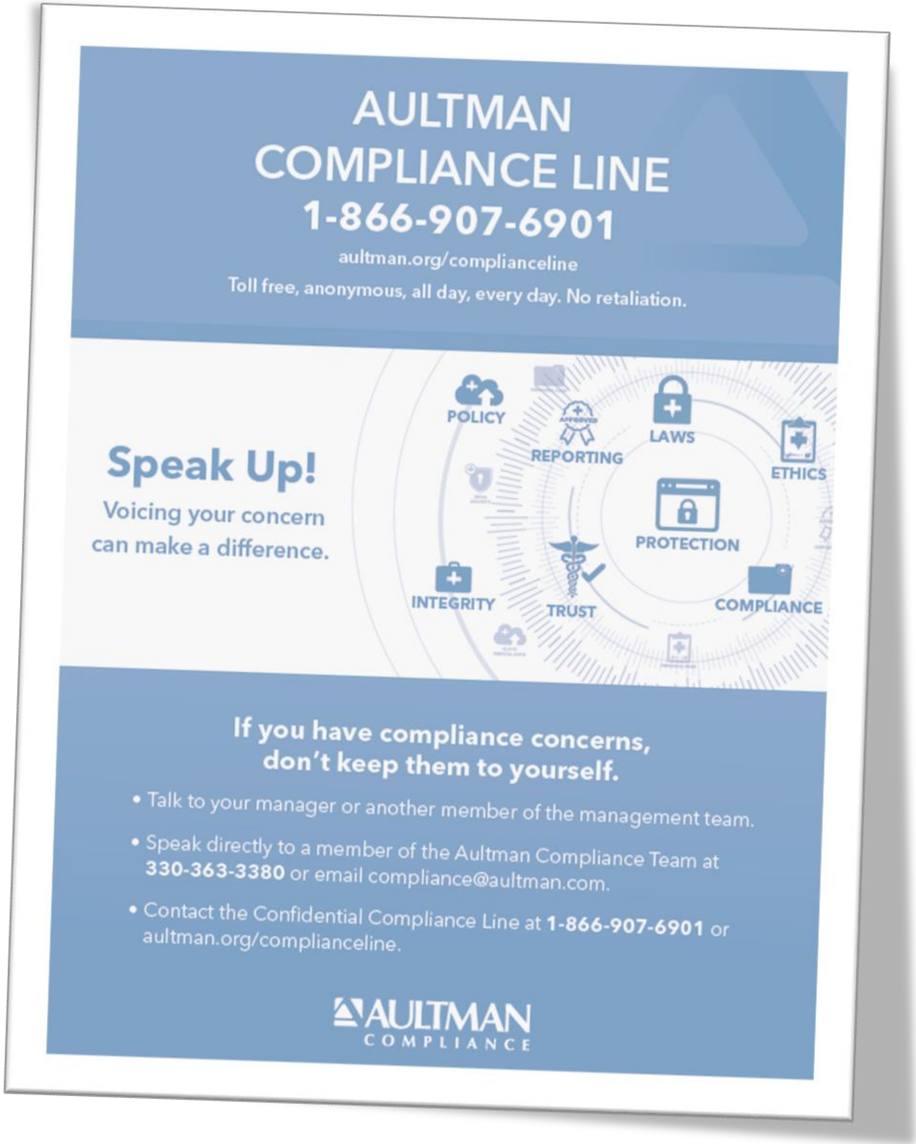
- Discuss concerns with your manager or another member of the management team.

- Contact the **Aultman Compliance department**:
  - ❖ 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 Aultman Compliance department for investigation and resolution.)

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



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

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)
- Snooping / Unauthorized Access to Patient Information
- HIPAA Audits
- Pay Attention to Detail
- HIPAA Breach

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).

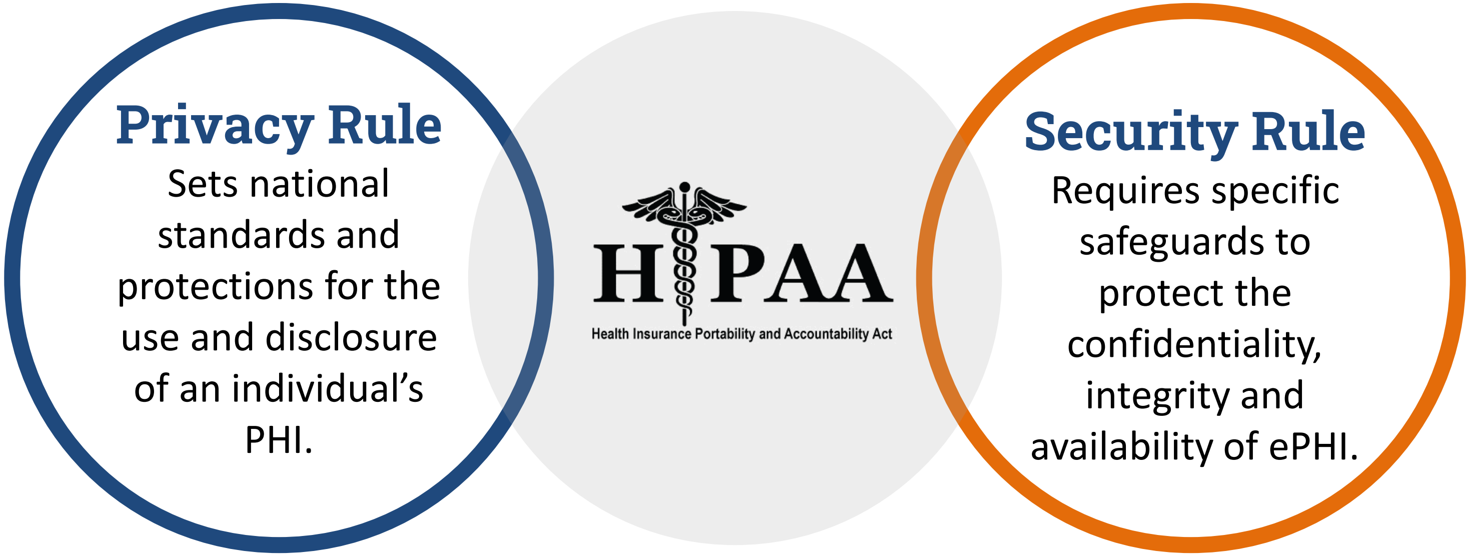
AULTMAN

Health Insurance Portability and Accountability Act

HIPAA

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 key parts:



Privacy Rule

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

Security Rule

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

Who Must Comply with HIPAA?

- All covered entities must comply with HIPAA. 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 healthcare, 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.

HIPAA Covers All Protected Health Information (PHI)

PHI is any past, present or future physical or mental health information that could identify a person, including payment information.

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.

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

Permitted PHI Use and Disclosure

Hospitals and physician offices use PHI. They also disclose it outside the organization for different purposes. Some examples include:

Use: The access to, or sharing of PHI, within Aultman.

- ✓ Doctors' orders for treatment
- ✓ Nurses' notes for quality review
- ✓ Patient registration

Disclosure: The release of PHI to any person or entity outside of Aultman.

- ✓ Public health reporting
- ✓ Claims submission to insurance companies for payment
- ✓ Accreditation organizations (for example: The Joint Commission)

HIPAA requires a healthcare provider to have a legitimate treatment or business need to use or disclose PHI.

HIPAA
Minimum Necessary Standard

How can you protect PHI? **Only access and disclose the minimum amount of protected health information (PHI) for a job-related reason**. This is called the Minimum Necessary Standard.

- **It's simple: Accessing the medical records of yourself, your family, your friends, your neighbors or your co-workers for a non-work-related reason is <u>strictly prohibited.</u>**

Examples of following the minimum necessary standard:

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.

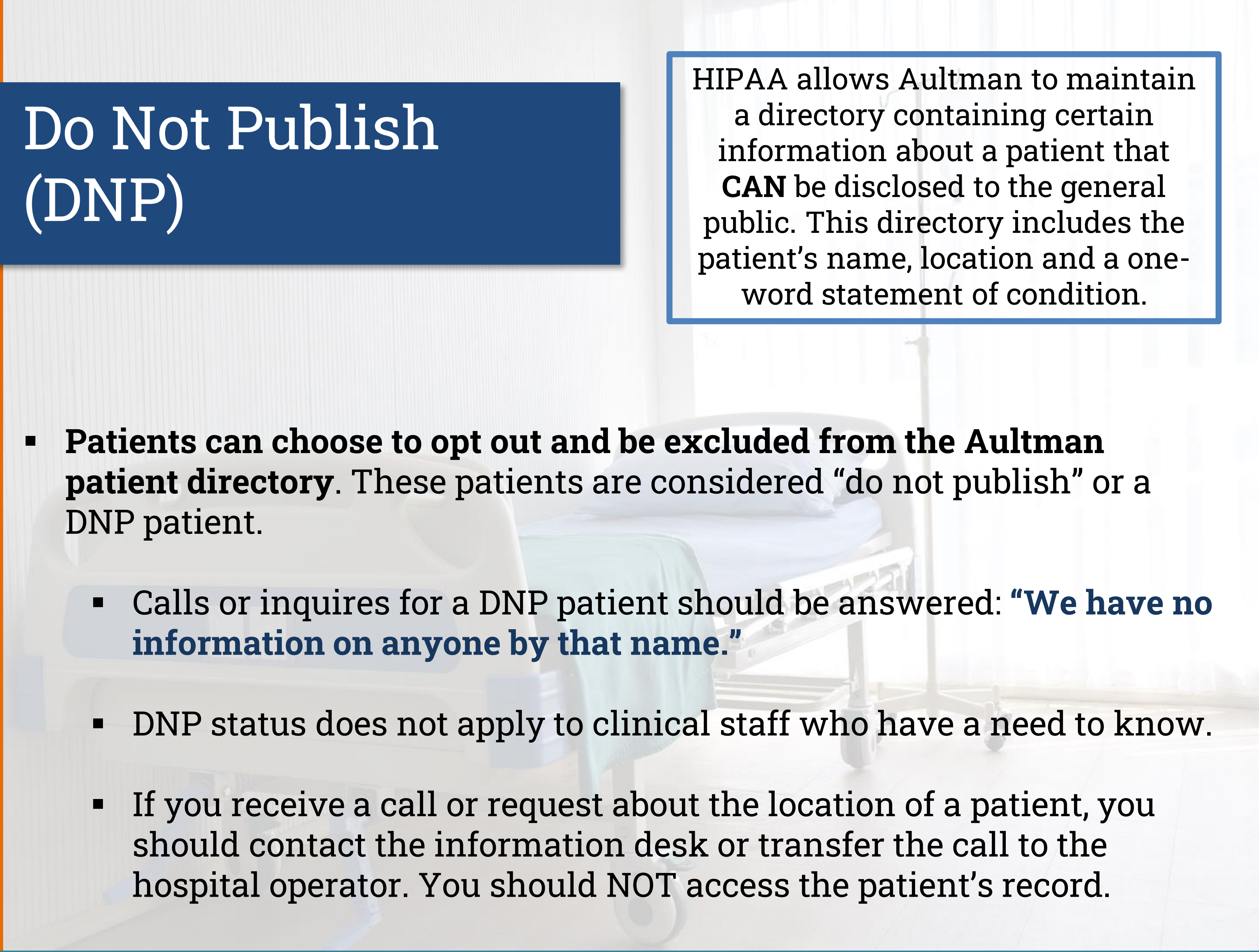
If a provider needs to know about a patient's family history, they should look in the patient's record but not the actual records of family members.

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.

To do so, you must:

- **Obtain patient approval before sharing PHI.**
  - Oral or written approval is acceptable.
  - This approval must be documented 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 to receive PHI.



Do Not Publish (DNP)

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.

- **Patients can choose to opt out and be excluded from the Aultman patient directory**. These patients 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."**
  - DNP status does not apply to clinical staff who have a need to know.
  - If you receive a call or request about the location of a patient, you should contact the information desk or transfer the call to the hospital operator. You should NOT access the patient's record.

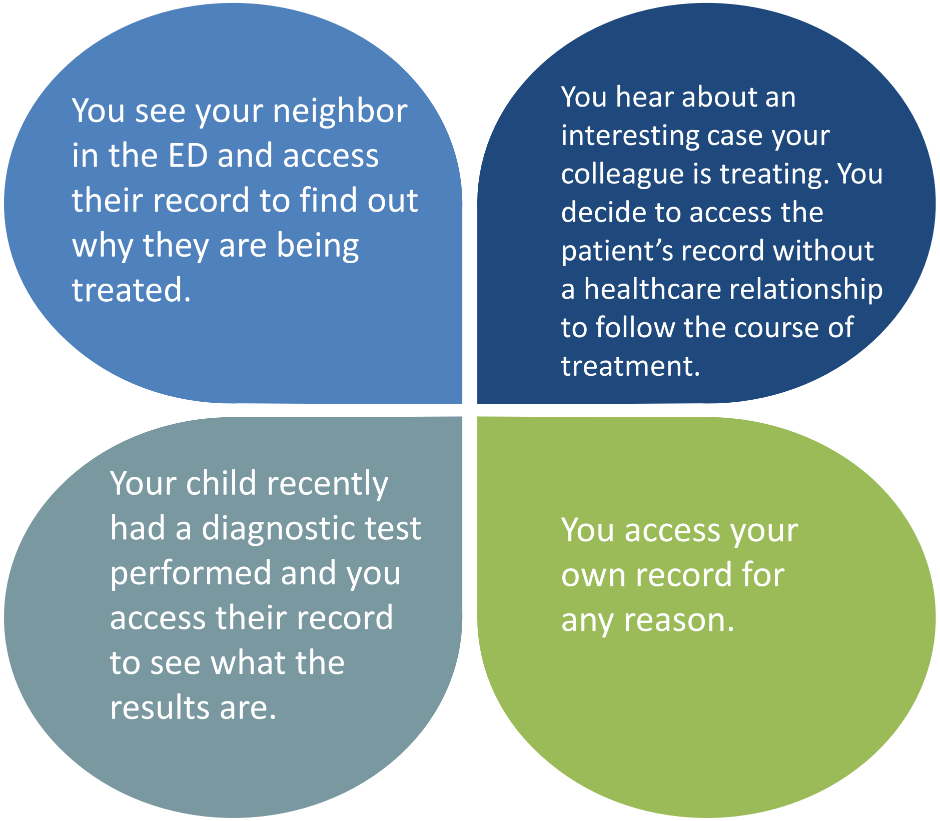
Snooping and Unauthorized Access

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:



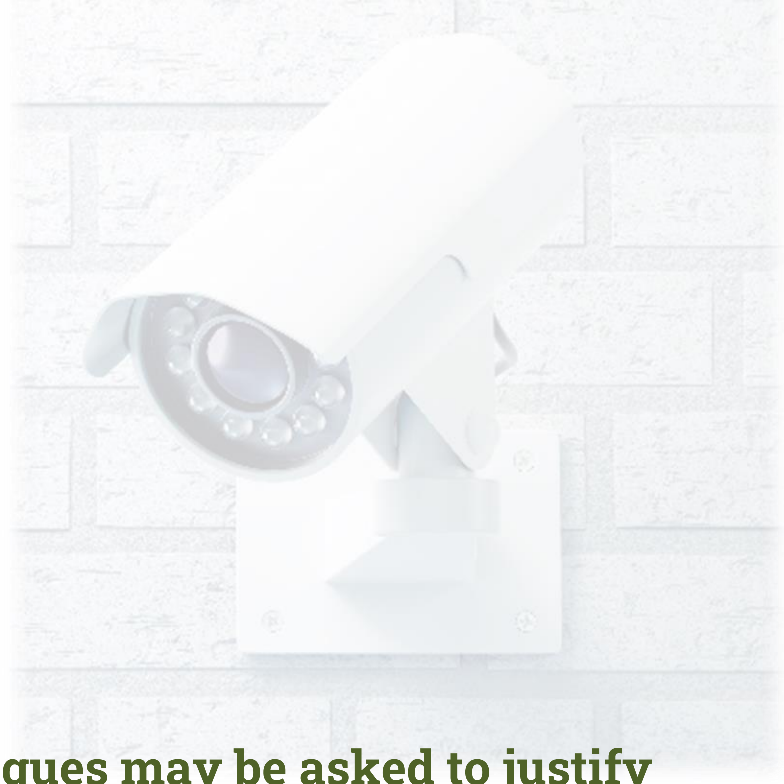
You see your neighbor in the ED and access their record to find out why they are being treated.

You hear about an interesting case your colleague is treating. You decide to access the patient’s record without a healthcare relationship to follow the course of treatment.

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 monitors and audits access to all electronic medical record systems, as required.

Audit reports show:

- **WHO accessed a record**
- **WHEN it was accessed**
- **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.

JUST BECAUSE YOU CAN ACCESS SOMETHING DOESN'T MEAN YOU SHOULD!

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.

HIPAA Breach

A HIPAA breach is an inappropriate access, acquisition, use or disclosure of PHI and can carry serious consequences.

Breaches occur when PHI is:

- Lost, stolen or improperly disposed of,
- Compromised when a colleague falls for a phishing email, downloads malware or grants bad actors access to our systems,
- Accessed inappropriately by colleagues who have no business reason to do so,
- Communicated or sent to someone who has no official need to receive it (i.e. gossip, social media posts, snooping).

Potential and suspected breaches or disclosures must be reported to Aultman Compliance immediately.

Topics:

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

Cybersecurity Awareness

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

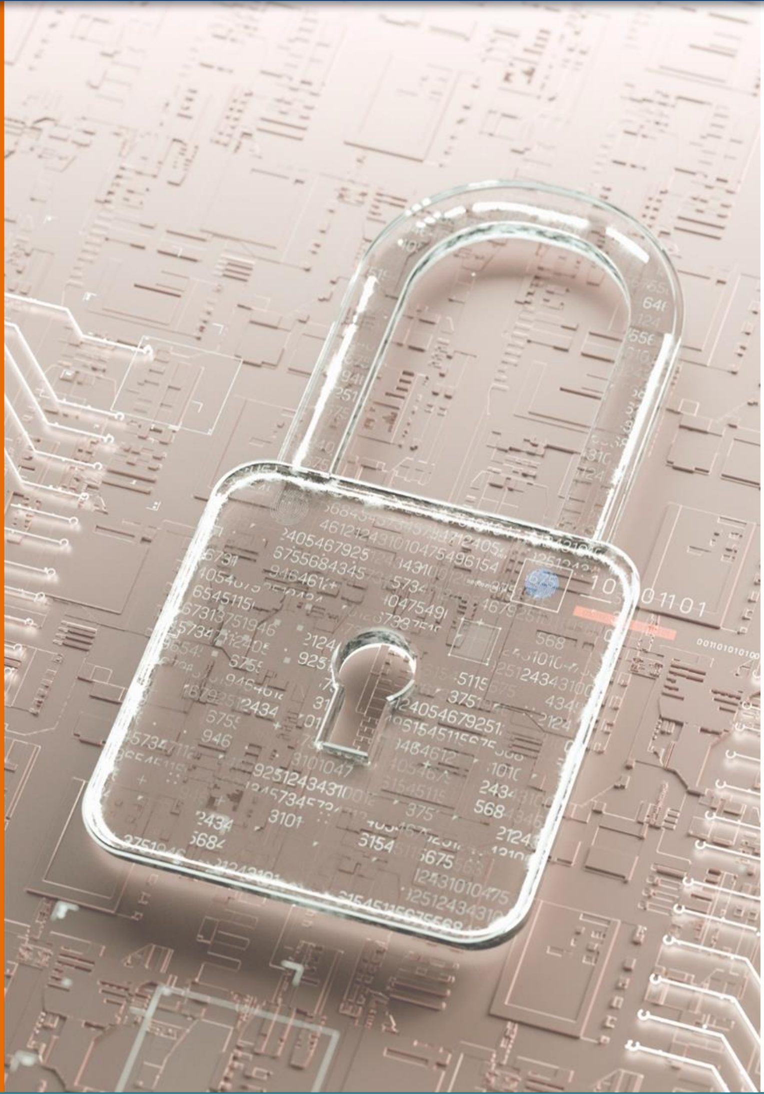
AULTMAN

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 a 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.

Securing Aultman Systems is Our Shared Responsibility



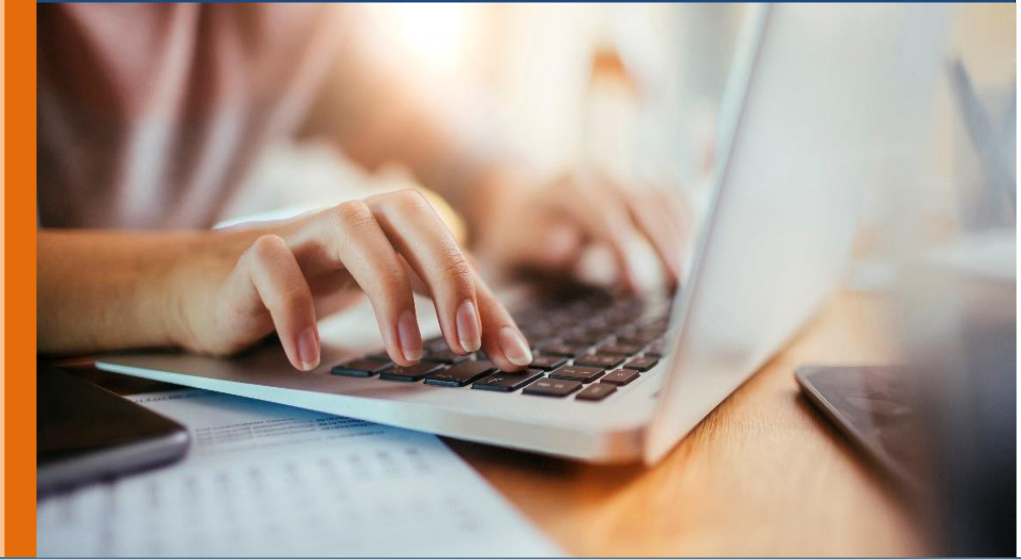
Remember:

- **NEVER** provide your Aultman username and password when asked in email or to access an email attachment.
- Even if you know the sender, if it is an unexpected attachment, check with IT before opening it.
- If something looks suspicious, seems odd or is unexpected, **report it** via the phish button. If it is legitimate, IT will let you know.
- If you enter your credentials in error, are notified someone's email was compromised or receive a suspicious phone call(s), **notify IT immediately at EPHIsecurity@aultman.com.**

The files we download from the internet can harbor behind-the-scenes computer viruses and spyware or open a “back door,” giving others access to your computer without your knowledge.

These viruses and spyware are called “malware.”

Colleagues are prohibited from using Aultman computer assets for personal use.



- **Stay Alert:** Don’t open unsolicited attachments. Only download files, apps and plugins from known trusted sources.
- **Be Smart:** Don’t download unknown software (especially free software), files or pictures. These files may be .exe or .vb files and may contain malware.
- **Be Diligent:** Don’t click on links or ads for software in email, pop-ups, instant messages/texts or social networking sites.

If you download a file or document that you suspect to be suspicious, please place a help desk ticket immediately or email ephisecurity@aultman.com.

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

- **NEVER** take pictures of patients or items such as X-rays, patient lists or computer screens with personal cell phones or devices.

- Texting of patient information should only be performed with Aultman approved platforms that are secure and encrypted.

Mobile Devices

When using a secure texting platform (STP), patient care information and orders can be shared among healthcare team members.

Aultman DOES NOT allow texting of patient care orders, regardless of the platform used.

Social Media

The information you learn as part of your work at Aultman is confidential and should NEVER be shared on social media.

Even if just one person can identify the patient you are posting about, the post is identifiable and may be a HIPAA breach.

What should you avoid?

- × Taking/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
- ✓ 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.