2020 HIPAA & Compliance Annual Education
Our 2020 HIPAA and Compliance education emphasizes HIPAA, the importance of electronic cybersecurity awareness and your role in keeping information safe. This education also covers the Aultman Compliance Program which supports our commitment to the highest standards of conduct, honesty and integrity in our business practices.

Privacy matters to all of us and especially to our patients. The HIPAA regulations are designed to protect patient privacy, provide patients with rights regarding their information and provide security over the technology used to collect, store, transmit and share our patients’ health information.

Compliance programs exist to identify risks 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 phone line or call us in compliance. 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.
The purpose of this education is to UPDATE and REFRESH your understanding of:

- The HIPAA rules and **PROTECTING OUR PATIENTS’** confidential information.

- **CYBERSECURITY AWARENESS** and your role in keeping information safe.

- Aultman’s **COMPLIANCE** Program.
Why is Patient Privacy Important?

Patients place their **TRUST** in us to protect their most private information.

If patients don’t trust us with their private information ...

- They may be reluctant to disclose important information that is vital to their care.
- They may go elsewhere to receive treatment.
- Our community reputation could be damaged.

Not only do we have a **legal duty** to protect patient health information, we have an **ETHICAL and MORAL** obligation as well.
What is HIPAA?

HIPAA is a federal law which:

- Regulates and sets standards for protecting patient privacy and confidentiality of Protected Health Information (PHI).
- Describes how we may use and disclose health information.
- Expands patient’s rights regarding their health information.
- Includes penalties for privacy violations.
**Protected Health Information** – 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 a patient.
- 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 screenings as condition of employment.
  - Disability insurance forms.
- Family Educational Rights and Privacy Act (FERPA) records.
- De-identified health information.
Uses and disclosures of PHI are permitted without patient authorization for the purposes of healthcare
T**reatment**, **Payment** & **Operations** (TPO).

<table>
<thead>
<tr>
<th>Treatment</th>
<th>Payment</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Provision or coordination of care by or among health care providers.</td>
<td>- Coverage determinations</td>
<td>- Case management, care coordination.</td>
</tr>
<tr>
<td>- Referral of patients by one provider to another.</td>
<td>- Billing, claims management and medical data processing.</td>
<td>- Audit / compliance activities.</td>
</tr>
<tr>
<td>- Coordination of health care or other services among providers and authorized third parties.</td>
<td>- Review of health care services for medical necessity, etc.</td>
<td>- Conducting or arranging for medical review, legal services or necessity.</td>
</tr>
</tbody>
</table>
What can I tell my patient’s friends and family?

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.
- Use the Privacy Communication tab in Cerner or paper form.
- Patient may change his/her mind at any time.

Use professional judgment when patient is unconscious or incapacitated.

- Only disclose the minimum amount of information necessary to do your job.
- Family & friends should be actively involved in care in order to receive PHI.

When in doubt, do not disclose information!

Remember, you can consult your manager or compliance for guidance.

Learn more by reading Aultman’s Sharing PHI with Family, Friends, or Others policy.
Aultman Patient Directory

HIPAA allows Aultman to maintain a directory containing certain information about a patient that **CAN** be disclosed to the general public.

- This information includes: Patient’s name, location, and a one-word statement of condition.
- At the time of registration, the patient will be informed about the information included in the directory and may choose to restrict the information, restrict to whom it is disclosed or opt-out of being included in the directory completely.

**DNP**

Patients choosing to opt out and be excluded from the Aultman patient directory are considered Do Not Publish or a DNP patient.

- No information regarding his/her presence in the facility or condition will be released without their specific authorization.
- 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 to the general public.
- The patient may share information on their own with anyone.
- No flowers and/or mail will be delivered to DNP patients.
- Calls or inquiries for a DNP patient should be answered: **“We have no information on anyone by that name.”**

Learn more by reading Aultman’s [Do Not Publish](#) policy.
Snooping is when a workforce member accesses the record of an individual for a reason that is not job related, regardless of intent.

Examples of snooping may include:

- 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.

Aultman policies DO NOT PERMIT workforce members to look up their own medical information, or that of family, friends, co-workers or patients of interest.

One way to appropriately access your health information is through the patient portal, Aultman OneChart.

Learn more by reading Aultman’s Workforce Access to Personal PHI/Records policy.
Minimum Necessary Standard

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

- Looking up 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.

Examples of utilizing 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.
- A provider may need to access a patient’s family history in the patient’s record but should not go into the actual records of the family members.

Learn more by reading Aultman’s Minimum Necessary Requirements for Using, Requesting, and Disclosing Information policy.
Aultman takes patient privacy seriously and proactively audits and monitors our workforce member’s access to patient records.

Inappropriate access may result in disciplinary action. It also may require reporting to the patient and to the government.

Aultman uses a software called **FairWarning** that allows us to:

- Conduct random audits of employee access.
- Investigate any patient complaint regarding HIPAA.
- Run reoccurring specialized reports, such as:
  - Co-worker snooping
  - Household snooping
  - Self access
  - Snooping on a manager
  - VIP snooping

Consider this a

We can see **WHO** accessed a record, **WHEN** it was accessed and **WHAT** information was viewed.
Common HIPAA Violations

- Discussions of patient information in a public place or with inappropriate, unauthorized individuals.

- Print or electronic information left exposed where visitors or unauthorized individuals can view it.

- Records accessed without need to know.

- Sending PHI to the wrong place.
Consequences of a HIPAA Breach

With each HIPAA violation that occurs, a risk assessment is conducted. If the violation rises to the level of a reportable breach, that means Aultman must notify the patient and the government.

The penalties are real ... and serious!

You may receive discipline ranging from:

- WARNING
- SUSPENSION
- TERMINATION

- Aultman can be fined up to $1.5 million for a HIPAA violation.
- You may also be held personally responsible.

Aultman’s disciplinary process is outlined in the Employee Handbook.
It Happened at Aultman...

An access audit revealed an employee accessed their co-worker’s records. This employee was SUSPENDED.

A patient presented to the ED with an orthopedic injury. An employee took a picture of a patient’s X-ray with a personal cell phone and posted it to social media. This employee was SUSPENDED.

A workforce member provided their Aultman login credentials to another workforce member to investigate an issue. This employee was SUSPENDED.

A patient was sent home with another patient’s discharge instructions.

Aultman Security accompanied the employee responsible to RETRIEVE THE DOCUMENTS from the patient at home.

An employee left their Aultman issued laptop and work bag in their locked car in plain sight in a public parking lot. A thief used a hammer to break into the car and stole the items. The user’s login credentials were written on a sticky note affixed to the laptop. Quick action prevented inappropriate system access.

A workforce member used their personal cellphone to place a video call during their shift in a clinical area. A patient’s image was captured and shared without consent. This workforce member LOST THEIR JOB.

Two Aultman workforce members fell victim to phishing and provided their credentials to an attacker. Unknown individuals gained remote access to their email accounts and used them to send subsequent phishing emails. A review of 8,500 emails in the compromised email accounts revealed that some contained PHI in the form of conversations and attachments. This breach was reported to 36 patients and to the government.
The HIPAA Privacy and Security Rules DO NOT change in an Emergency Situation

Aultman must continue to implement reasonable safeguards to protect patient information from intentional or unintentional impermissible uses and disclosures of PHI.

Some of these safeguarding efforts include:

- Increased auditing and monitoring of access to patient records and patient information leaving Aultman.

- Increased workforce education on privacy and security:
  - Reminders included every Tuesday and Thursday edition of the Aultman Today.
  - Working remotely from home reminders.
  - Video conferencing security.

- Telehealth privacy and security.

- Monitoring for fraud schemes.

- Responding to reports of staff and patient compliance concerns.
Mobile Devices

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

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

The Joint Commission and CMS prohibits the texting of patient care orders, regardless of the platform utilized.
Even though we increasingly lead our lives on social media, you need to be careful about anything you post online that might expose any patient information.

**Social Media and Patients … A Dangerous Interaction**

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

### 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 on social media any patients you met through work.

### Remember...

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

Social media posts with PHI can be punished as privacy breaches.

Source: Beazley Breach Solutions

Learn more by reading Aultman’s [Social Media Policy](#).
How to Send a [SECURE] Email

- Encryption protects the information contained in the email from unauthorized viewing by hackers.

- All emails sent to another Aultman email are secure.

- Emails containing patient information or other confidential information that are sent outside of Aultman must be encrypted.

- To encrypt an email from an @aultman.com address, type [SECURE] anywhere in the subject line.

- The brackets [ ] must be included, and the word “secure” is not case sensitive.
Recycling is great. But not for passwords

Using the same password for different accounts is tempting – like having one handy key that opens every lock you use. But reusing passwords is not the solution.

Compromised passwords are one of the leading causes of data breaches, and reusing passwords can increase the damage done by what would otherwise be a relatively small incident.

Cybercriminals know that people reuse credentials and often test compromised passwords on commonly used sites in order to expand the number of accounts they can access.

For instance, if you use the same password for your Aultman email as for Amazon or your gym membership, a breach at one of those companies puts your all your accounts at risk.

Before reusing a password for different accounts, especially across work and personal ones, think of all the data that someone could get into if they got that credential.

Source: Beazley Breach Solutions
Password Tips

• Use separate passwords for work and personal accounts.

• Avoid words that can easily be guessed by attackers like “password” or “September2020,” or predictable keyboard combinations like “1234567,” “qwerty,” or 1q2w3e4r5t.”

• Longer is stronger. Use passphrases rather than passwords. Passphrases could include several random words like “Highway owl purple elephant” or could be taken from favorite song lyrics or books.

• Add some complexity with capitalization or special characters. “Fido!sAnAwesomeDog” is a stronger password than your pet’s name.

• Just adding numbers or special characters at the end of a word doesn’t increase security much, because they’re easy for software to guess.

• Avoid words like your kids’ names that could easily be guessed by coworkers or revealed by a few minutes of online research.

Source: Beazley Breach Solutions

Learn more by reading Aultman’s Password Security Policy.
1. Secure your space
Don’t leave sensitive documents out when away from your workspace. Lock them away when you leave your desk, and if you can’t, get them out of sight.

2. Stay aware of your surroundings
Pay attention to tailgaters, shoulder surfers and strangers. If you see a stranger in the office without a badge or ID, direct them to the security desk.

3. “For your eyes only”
Label documents and files as sensitive, private or confidential so people can understand how they should be handled. If you discover sensitive information that’s not properly protected, report it immediately.

4. Use stronger passwords
Longer is stronger. Instead of easy-to-crack passwords like Passord1!, use a passphrase, like 1 Red Elephant Balloon Maker?, or a sentence you can easily remember.

5. Don’t mix business with pleasure
When you use work email for internet play, you give the bad guys more opportunities to get in. Use work email for work, and your own email for personal matters.

6. Secure your personal devices
If you have a work laptop or device, use it only for work and don’t expose company assets to unnecessary risks.

7. Don’t get “attached”
Word documents and PDFs can hide exploits sent by a hacker. If you get an unexpected or strange email attachment from someone you know, call to check whether it’s legit.

8. Use it or lose it
If you find a stray USB drive or removable hard drive, don’t plug it in. It’s an old hacker trick to litter the area around an office with infected USB devices. Don’t plug in a hacker’s weaponized USB, send it to IT!

9. Beware of Wi-Fi eavesdropping
Bad actors can easily impersonate known Wi-Fi connections using a cheap device that can kick you off a router and fool your device into happily accepting a faster connection. Don’t ignore browser warnings. Use a secure virtual private network (VPN) or tether to your own phone or hotspot.

10. Travel smart
When working remotely, you’re not protected like at the office. Privacy screens help keep your work private. Lock your computer when you’re not using it, and lock up laptops and sensitive documents safely when you’re done for the day. Take sensitive documents back home with you if you can’t dispose of them properly.

Source: Beazley Breach Solutions
How to Spot a Phishing Email

Spelling and bad grammar
If you notice mistakes in an email, it may be malicious.

The hyperlinked URL is different
Hover your mouse over the address in the “from” field to see if the website domain matches that of the site the email should have originated from.

Call to action
Often they will trick you into clicking on a link to reactivate your account or to remove a hold. Don’t click on the link, but instead log onto your account in question directly through their website.

You Won!!
A common scam is to send an email that says you won a prize for a contest you never entered.

Payment Invoice
Scammers posing as well-known companies will email a phony invoice showing that you’ve recently bought an item. The email prompts you to click the link if you did not authorize the purchase. Be suspicious if a business or organization asks you to click on a link then asks for your username or password.
If you feel you have received a phishing email or fallen victim to a phishing scheme, please notify our IT Security Department IMMEDIATELY by:

- Reporting the message using the Report Message button located in the home ribbon at the top of your Office 365 screen.
- Submitting a Help Ticket located on the Employee Portal.

or
Healthcare compliance is an expectation of all Aultman workforce members.
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 non-compliance.
- Provides a method for employees to report potential problems.
- Serves as a resource to resolve compliance issues.

Aultman’s Compliance Program strives to:

- **PROTECT** our organization, workforce members and customers.
- Preserve the level of **INTEGRITY** that Aultman is known for as a highly reliable organization.
- Promote the continued effort to **DO THE RIGHT THING**.
As an Aultman workforce member, what is expected of me?

Follow Aultman’s Code of Conduct.

Carry out your job duties with **INTEGRITY** and **HONESTY**.

Know the laws and regulations that apply to your job.

Exercise good judgment and do the right thing when performing your job.

Report suspected compliance concerns or problems to the Compliance Department.
Fraud, Waste, and Abuse can occur in many different formats.

For example...

Billing for services not furnished or that are medically unnecessary could be considered FWA.

If you have a concern or question about how things are being done, it is important that you report your concern.

An estimated 10% of Medicare costs are wrongly spent on fraud, waste, and abuse.

The government devotes substantial resources towards preventing and detecting FWA.
Medicare Conditions of Participation (CoP)

What:
Federal regulations with which healthcare organizations must meet to participate in and receive funding from the Medicare and Medicaid programs.

Who:
Healthcare organizations, like Aultman, participating in the Medicare and Medicaid programs.

Why:
The CoPs are intended to protect patient health and safety and to ensure that high quality care is provided to all patients.

CoP Knowledge is Critical

- Medicare/Medicaid payments account for 70% of Aultman payor mix.
- CoP Non-Compliance leads to:
  - Financial penalties.
  - Additional gov’t surveys.
  - Removal from program.
- Impacts participation with other insurers.
- Compliance can be demonstrated by accreditation from:
  - The Joint Commission.
  - HFAP.

CoPs are published in the Code of Federal Regulations (CFR) by section number and title (example: §482.1 Basis and Scope)
How do I 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](https://www.aultman.org/complianceline).

Employees reporting in good faith will not be subject to retaliation.
Aultman will not tolerate retaliation, harassment, discrimination or adverse action against any member of its workforce who makes a good faith complaint or report to a supervisor, manager, the Compliance Office, Human Resources, Legal Affairs, an authorized agency or a law enforcement entity.

Aultman encourages the reporting of concerns, problems and opinions on issues without fear of retaliation.

Compliance Concerns include but are not limited to:

- Aultman Policy/Code of Conduct compliance.
- Violations of confidentiality
- Quality of care or patient safety.
- Billing and coding.
- Accounting and auditing.
- Violations of law and regulations.
- Suspected or actual criminal conduct.

Learn more by reading Aultman’s Non-Retaliation policy.
KEYS TO SUCCESS

HIPAA & Compliance

- Use your HRO Tools to Prevent and Detect non-compliance.
- Always Safeguard & Protect patient information.
- Contact your manager or Compliance to Report & Resolve issues.
- Carry out your job duties with Integrity & Honesty.
- Make an Impact & Promote a culture of compliance at Aultman.
Questions?

Kelly Martinelli  
Physician Practice Group Compliance Officer  
Ext. 46493 or 330-433-1493  
kelly.martinelli@aultman.com

Karen Wulff  
Integrated Health Collaborative  
Compliance & Privacy Officer  
Ext. 33115 or 330-363-3115  
karen.wulff@aultman.com

Brenda Greer  
Aultman Alliance Community Hospital Liaison  
Ext. 33959 or 330-363-3959  
brenda.greer@Aultman.com

Janice Cooper  
Director, IT Security  
Ext. 33403 or 330-363-3403  
janice.cooper@aultman.com

Direct questions regarding **Systems and Technology Security** to:  
[EPHIsecurity@aultman.com](mailto:EPHIsecurity@aultman.com) or  
submit a [Help Desk Ticket](https://aultman.com) via the Employee Portal.
HIPAA regulations require Aultman to provide ongoing compliance education for all employees 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 employee must complete the post-test and answer 80% of the questions correctly.

Please proceed to the post-test now.