



Annual Provider, Contractor, Vendor Representative, and Volunteer Compliance Education - 2024

#1 Privacy Reminders	#2 AH Compliance Program	#3 Code of Conduct
-------------------------	-----------------------------	-----------------------



#1 Privacy Reminders



HIPAA: The Health Insurance Portability and Accountability Act (HIPAA) is a federal law that requires Volunteers to:

1. **Protect the privacy** of patient information
2. **Secure patient health information** in physical and electronic form
3. **Adhere to the “minimum necessary”** standard for use and disclosure (i.e., sharing) of patient health information

HITECH: The Health Information Technology for Economic and Clinical Health Act

- ✚ **HITECH Requires Adventist Health to** report breaches of patient privacy to the Secretary of the Department of Health and Human Services.

Additional State Laws

- ✚ **Many states have additional laws** establishing obligations and penalties relating to the security and privacy of patient information.
- ✚ **For example, California law requires** licensed healthcare facilities to report breaches to the California Department of Public Health (CDPH) and to the affected patient(s) within **15** business days of discovery.




Adventist Health Policies


Adventist Health privacy policies apply to **ALL** written, verbal, and electronic information.

Patient privacy and confidentiality are important to Adventist Health because:

1. **Patient confidentiality** is essential to the development of trust between providers and patients.
2. **Patients have a legal right** to control who sees, accesses or hears their protected health information (PHI).
3. **Patients must be able to expect** that information about their health is kept private, unless there is a compelling reason that it should not be (i.e., for treatment, payment or healthcare operations).
4. **Without patient privacy**, patients would be hesitant to reveal sensitive information about themselves.
5. Providers and Adventist Health workforce members can be held personally liable for violating patient privacy laws. This includes fines and penalties (e.g., jail time).

 This means that communications with or about patients need to be kept private and **limited to those people who need to know the information for treatment, payment, or healthcare operations purposes**

How the Laws Apply to You

1. **Patient information** that you **see, hear, or read** during the course of performing your duties, **cannot** be shared with anyone unless the sharing of information is necessary to fulfill a job-related purpose and the recipient has a job-related need to know.
 This includes your co-workers, other patients, visitors, your family and friends, or anyone else who may ask you about information.
2. **Protecting patient information** is a responsibility that the entire workforce shares, including providers, regardless of whether you are directly involved in the care of patients.

Use of Social Media

1. **Do not share** any patient information on social media that is acquired through your work at Adventist Health, even if the information is public.
2. **Posting patient information without** appropriate authorization from the patient is a violation of a patient's **right to privacy and confidentiality**.
3. Even if you do not include the name or other identifying information in your communication, it still may **be identifiable to others**.

What is PHI?

Protected Health Information (PHI) includes:

- Names
- Dates relating to a patient:
 - birthdates
 - dates of medical treatment
 - admission and discharge dates
 - dates of death
- Other:
 - telephone numbers:
 - addresses (including city, county, or zip code) fax numbers and other contact information
 - Social Security numbers
 - Medical records numbers
 - Photographs
 - Finger and voice prints
 - Any other unique identifying number
 - Bills
 - Claims
 - Prescriptions
 - Data
 - Lab results
 - Medical opinions
 - Appointment histories

Ways to Protect PHI



1. **Be aware** of your surroundings.
2. **Keep information** confidential.
3. **Do not share patient information** with unauthorized individuals, even if the information is de-identified.
4. **Do not view information** out of curiosity or concern.
5. **Do not post patient information** of any kind on social media.
6. **Lock computer screens** when left unattended.
7. **Verify patient identifiers prior** to mailing patient information to ensure that it gets to the right person at the right place.
8. **Do not leave patient information** on answering machines.
9. **Dispose of PHI** only in appropriate shred bins, not regular trash cans.
10. **Do not share** your username and password with any other individual for any reason.



Access to Protected Health Information and EHR Access Auditing, Adventist Health Policy No. 12018

1. The privilege of access and user credentials (i.e., usernames and passwords) *are* provided to physicians and other Adventist Health workforce members **for business-related purposes only**. Business purposes include, but are not limited to, the treatment of Adventist Health patients.
2. Physicians and other Adventist Health workforce members may be patients within the facility for which they work or do business. Similarly, your family members and friends may additionally be patients within the facility where you work. As a patient you have the **same rights to PHI as the general patient population** and, therefore, care must be taken to ensure that these individuals are not provided greater rights to information than patients are entitled to.
3. To access personal information or PHI, such as medical records or test results, **you may contact the ordering provider, sign up for the MyAdventistHealth patient portal or obtain information from Health Information Management or Medical Imaging**. It is **not permissible to access** information **for personal reasons** utilizing your **AH user credentials**.
4. **AH has the right** (and is required by law) **to conduct audits** of electronic systems containing patient medical information **to ensure that any access** to patient information was performed with **appropriate business need to know**.
5. **Non-compliance** with this policy by physicians will be addressed by established facility **medical staff review processes**, all others will be addressed by Human Performance or the relevant contract.

Don't Get Phished

1. Business email compromise is one of the most financially damaging online crimes, exploiting the fact that we rely on email to conduct personal and professional business.
2. **Phishing** is when scam artists send official-looking emails, **attempting to fool you** into wiring money or misdirecting payments, **disclosing your AH username and password** or other personal information such as banking records or account numbers, social security numbers, etc. by replying to the email or entering the information into a fake website.
3. **Malicious software can infiltrate company networks** and gain access to legitimate email threads about billing and invoices. That information is used to time requests or send messages, so recipients or financial officers do not question payments. **Malware also lets scammers gain undetected access to a victim's data**, including passwords and financial account information.
4. How to protect yourself:
 - **Identify the sender.** Do you know this person? Were you expecting an email from this person or does it fit in with your job role? If not, it is probably suspicious. Legitimate, responsible companies including, **Adventist Health, will never solicit personal information or user credentials over email.** Never reveal personal or financial information in response to an email request to verify account information, etc. no matter who appears to have sent it.
 - **Reply-to.** If the Reply-to address is different from the sending address, this should raise your suspicion for the whole message. Carefully examine the email address, URL, and spelling in any correspondence. Scammers use slight differences to trick your eye and gain your trust.
 - **Links and Attachments.** If you were not expecting an attachment or a link, and you do not know the sender, do not open it! If you are not sure, check with the sender by phone (don't use a phone number in the email), otherwise report it to the Information Security Department by forwarding the email to Security@ah.org.
 - **Grammar and Tone.** While phishing scams are becoming more sophisticated, some malicious emails sent have poor grammar, punctuation and spelling. In addition, you should know how your colleagues communicate. Does this message sound like them? If not, it is probably malicious. Be wary of any emails trying to cause certain emotions, such as urgency or fear. Unusually short deadlines create a false sense of urgency to act. Attackers employ this technique in an attempt to confuse the recipient. Similarly, threatening recipients with negative consequences like threatening to shut off accounts or legal action are common tactics to generate a response.
 - **Be careful what you share online or on social media.** By openly sharing things like pet names, schools you attended, links to family members, and your birthday, you can give a scammer all the information they need to guess your password or answer your security questions.

- **Set up multi-factor authentication.** Set up multi-factor authentication (MFA) on any account that allows it, and **never disable it.** MFA increases account security by requiring multiple forms of verification to prove your identity when signing into an application. When you require a second form of authentication, such as a cell phone or fingerprint scan, a scammer will have difficulty duplicating or obtaining the additional identification needed to compromise your account.
5. All physicians and AH workforce members who receive a suspicious email should report it immediately to the AH Information Security Department at Security@ah.org. Even if you are not sure, it is better to have the message reviewed by an expert. In addition, just because you may think the email is an obvious phishing scam, it may not be so obvious to others.

Sanctions for Violating Privacy Rules

1. **Adventist Health has a workforce sanction policy** for members of our workforce who violate patient privacy and privacy/security policies. Refer to Lucidoc policy 10239, Privacy and Security Disciplinary Action Policy.
2. Potential **civil and criminal penalties** for violating HIPAA privacy or security rules, may include large fines and up to 10 years in prison.
3. **These penalties** can be levied against you, as well as Adventist Health.

Patient Privacy

- ✚ **We must all work to** honor and protect the privacy of our patients and to protect the confidentiality and integrity of our patient's protected health information.
- ✚ **It is professional practice** – pure and simple – but it is also federal and state law

2. Adventist Health Corporate Compliance



Eight Elements of the Corporate Compliance Program

1. **Code of Conduct** – explains Adventist Health’s expectations of ethical behavior for workforce members
2. **Compliance Officers**¹ – specifies that the Corporate Compliance Program is overseen and managed by the Corporate Compliance Officer and the Local Compliance Officers at each facility
3. **Policies** – sets Adventist Health’s expectations and requirements
4. **Training** – provides ongoing training on compliance topics
5. **Reporting**¹ – provides ways to report compliance issues or concerns
6. **Enforcing** – investigates and corrects compliance issues
7. **Auditing** - tests business activities to ensure the program is operating properly
8. **Risk Assessments** – tests business activities to ensure the program is operating properly

¹ The Code of Conduct, Compliance Officer List, Privacy Official list, and compliance reporting forms are available at: <https://www.adventisthealth.org/patient-resources/compliance-information/>

Greatest Compliance Risk Areas for AH:



1. IT Security
2. Patient Confidentiality/Privacy
3. Physician Contracts
4. Home Care
5. Laboratory
6. Health Information Management (HIM)
7. Coding
8. Patient Financial Services (PFS)
9. Hospital-Based Outpatient Clinics
10. Adventist Health Physician Network (AHPN)
11. Rural Health Clinics
12. Patient Identity Protection
13. Pharmacy 340B Drug Pricing Program

3. Code of Conduct



AH Code of Conduct

We have a code of ethics² and expect all dealings with AH to be performed with the highest level of honesty and integrity.

Federal and State False Claims Acts

Federal and State False Claims Acts prohibit any person or entity from submitting a false record or statement or approval.

The Penalties for violating Federal or State False Claims Acts include:

1. **Civil Monetary Penalties** of up to \$11,000 for each false claim submitted
2. **Three times the amount of damages** that the government sustains because of the false claim.
3. **The costs of the legal action** brought to recover for the false claim.

A private citizen may file suit under the Federal and State False Claims Acts on behalf of the government if the citizen has direct and independent knowledge of the submission of a false claim.

The government will decide whether to:

1. Intervene (take over the case), dismiss, or settle the case,
OR
2. Let the private individual pursue the case on his or her own.

In either case, the person who initially filed the case may receive a portion of the amount recovered in either litigation or settlement of the claim.

²The Code of Conduct is available at: <https://www.adventisthealth.org/patient-resources/compliance-information/>

Your Corporate or Local Compliance Official can provide more information regarding the Federal and State False Claims Acts.



Whistleblower Protections

Both the Federal and State False Claims Acts prohibit employers from retaliating or discriminating against a person who, acting in good faith, investigates, reports, or assists in uncovering a false claim or statement.

A person who suffers discrimination or retaliation based on protected activities has the right to sue under both the Federal and State False Claims Acts. If the individual can prove that their employer retaliated against them for engaging in protected activity, the individual is entitled to be “made whole.”

The remedies may include the following:

1. **Reinstatement** of the employee to their position
2. **Two times** the amount of back pay
3. **Interest** on the back pay
4. **Compensation** for any special damages (including litigation costs and reasonable attorneys’ fees)

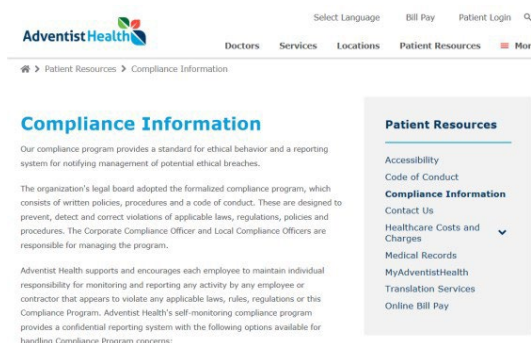
As noted above, it is the policy of Adventist Health and its affiliates that no one shall be punished solely on the basis that they reported what they reasonably believed to be an act of wrongdoing or a violation of the Adventist Health Corporate Compliance Program.

Your local compliance official can provide more detailed information.

Reporting Violations

You are encouraged to report violations or suspected violations to your supervisor, Corporate Compliance Executive, Local Compliance Official, or Facility Privacy Official.

- **Violations may be reported** to the Adventist Health Corporate Compliance **Hotline at 888.366.3833.**
- You may report **anonymously** (using AH Corporate Hotline number above)
- **Report using the AH Compliance Link:**
<https://www.adventisthealth.org/pages/compliance-information.aspx>



Attestation:

I acknowledge that I have received and read the Annual Provider, Contractor, Vendor Representative, & Volunteer Compliance Education.

Sign Name

Date

Print Name