Privacy

compliance

ETHICS

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 placed. (o)5.1 (n[)-1 (eh825 0 Td2er)22h825 0 oent gat the dy 749]T0 Tc 24.273**

[illegible]

ar

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

Greatest Compliance Risk Areas for AH:

1. **IT Security**

3. Code of Conduct

AH Code of Conduct

We have a code of ethics[2] 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

Attestation:

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

______________________________ ___________________

Sign Name **Date**

____

Print Name