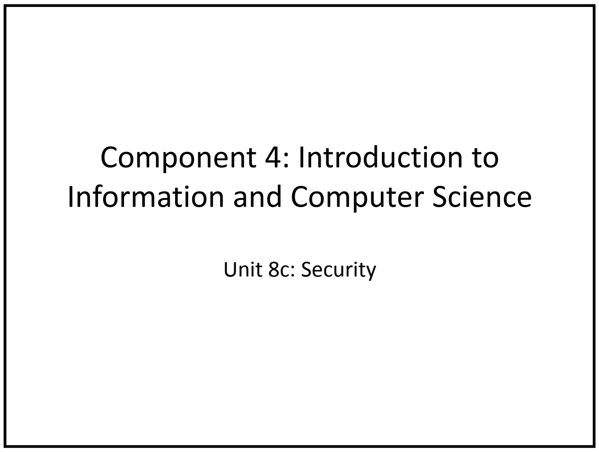
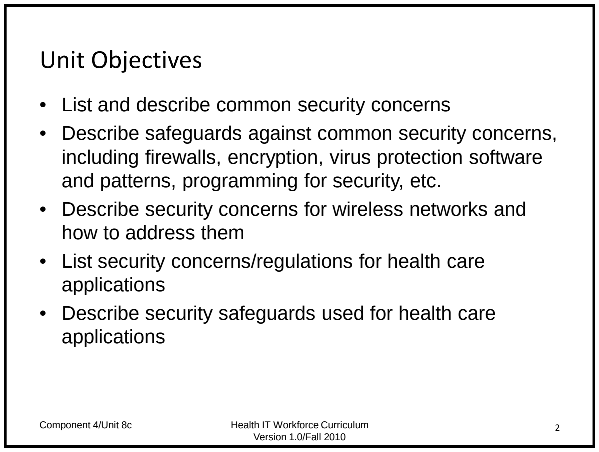


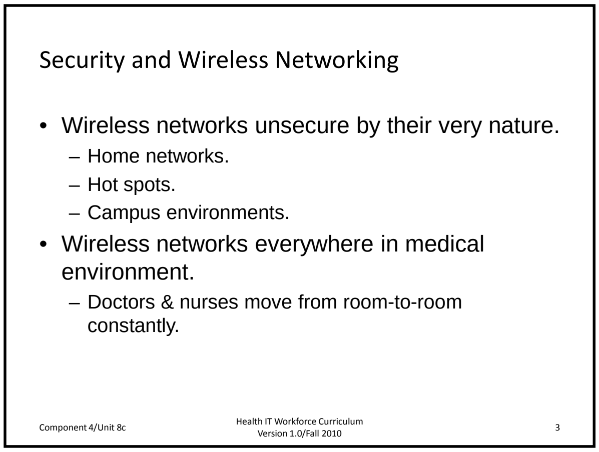
Component 4: Introduction to Information and Computer Science

Unit 8c: Security



Unit Objectives

- List and describe common security concerns
- Describe safeguards against common security concerns, including firewalls, encryption, virus protection software and patterns, programming for security, etc.
- Describe security concerns for wireless networks and how to address them
- List security concerns/regulations for health care applications
- Describe security safeguards used for health care applications



Security and Wireless Networking

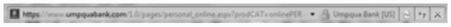
- Wireless networks unsecure by their very nature.
  - Home networks.
  - Hot spots.
  - Campus environments.
- Wireless networks everywhere in medical environment.
  - Doctors & nurses move from room-to-room constantly.

Wireless Device Security

- Wireless Access Points (WAPs) must be configured for security:
  - Change default password.
  - Select unique SSID.
  - Do not broadcast SSID.
  - Require WPA2 authentication.
  - Restrict access to known devices.
    - Can program MAC addresses into WAP memory.

Wireless Device Security (cont’d)

- Install digital certificates on sensitive devices.
  - Only devices with known/valid certificates can communicate on network.
  - Requires use of special servers.
  - Not usually for small offices.
    - The image shows a partial browser address bar with a valid bank certificate.
    - Click the gold lock to view the bank’s certificate.

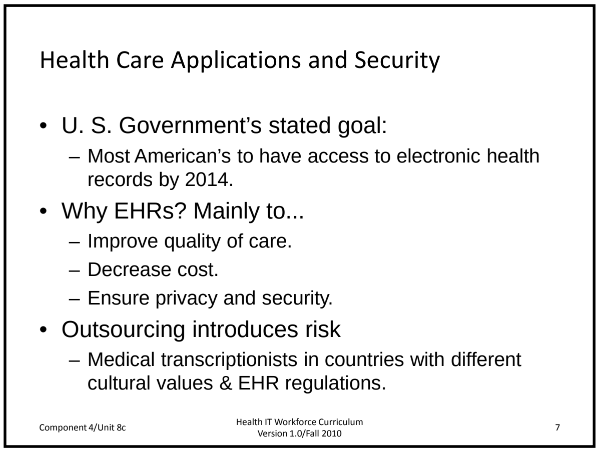


https://www.umpquabank.com/1.0/pages/personal_online.aspx?prodCAT=onlinePER

Umpqua Bank [US]

Wireless Device Security (cont’d)

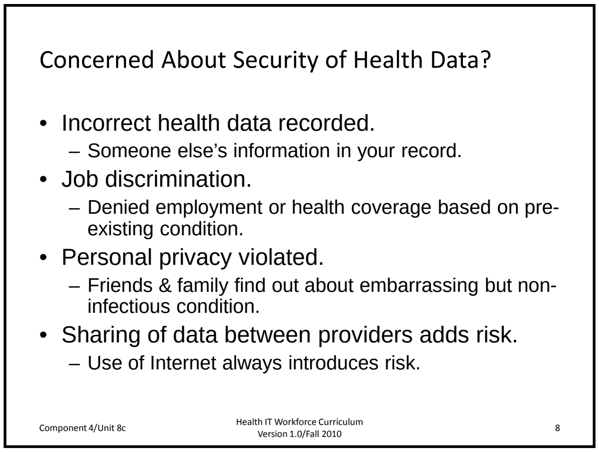
- Smartphones
  - All portable devices connecting to network need AV protection.
  - Do not use a portable device for sensitive transactions unless it is AV protected.
  - Do not open e-mail or attachments from unsolicited sources.
    - Known sources might be virus infected, meaning that they did not send the e-mail/attachment.
  - No exceptions.



Health Care Applications and Security

- U. S. Government's stated goal:
  - Most American's to have access to electronic health records by 2014.
- Why EHRs? Mainly to...
  - Improve quality of care.
  - Decrease cost.
  - Ensure privacy and security.
- Outsourcing introduces risk
  - Medical transcriptionists in countries with different cultural values & EHR regulations.

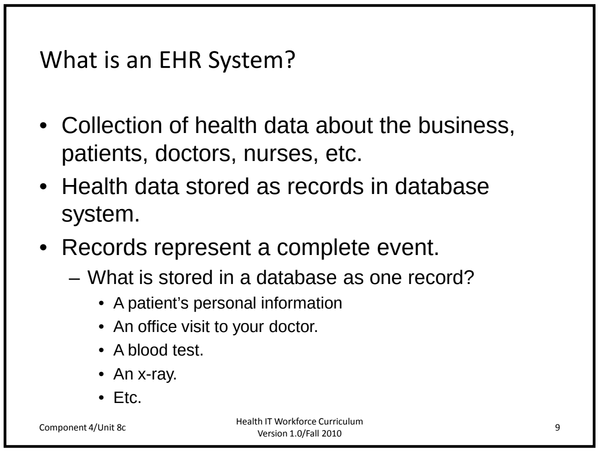
Component 4/Unit 8c Health IT Workforce Curriculum Version 1.0/Fall 2010 7



Concerned About Security of Health Data?

- Incorrect health data recorded.
  - Someone else's information in your record.
- Job discrimination.
  - Denied employment or health coverage based on pre-existing condition.
- Personal privacy violated.
  - Friends & family find out about embarrassing but non-infectious condition.
- Sharing of data between providers adds risk.
  - Use of Internet always introduces risk.

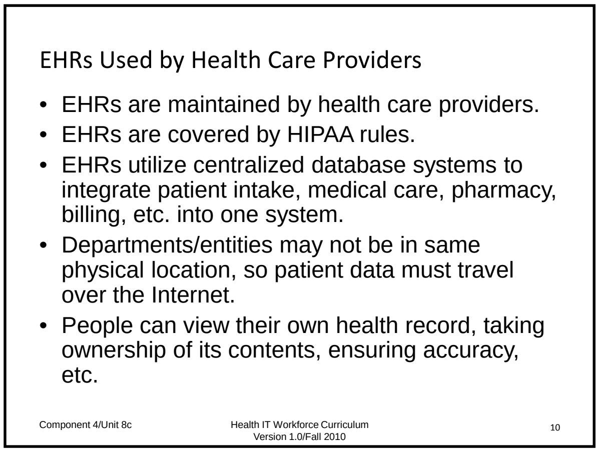
Component 4/Unit 8c Health IT Workforce Curriculum Version 1.0/Fall 2010 8



What is an EHR System?

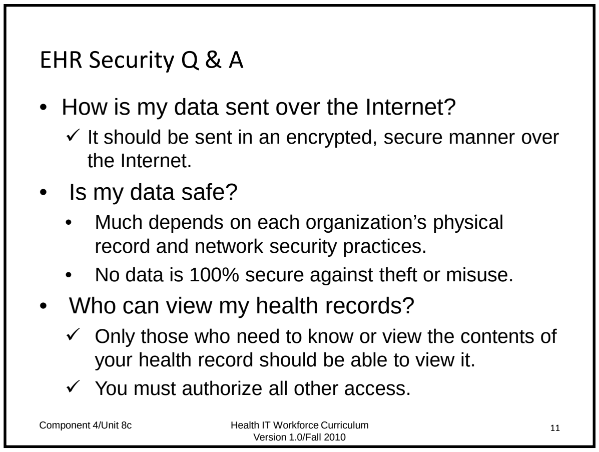
- Collection of health data about the business, patients, doctors, nurses, etc.
- Health data stored as records in database system.
- Records represent a complete event.
  - What is stored in a database as one record?
    - A patient's personal information
    - An office visit to your doctor.
    - A blood test.
    - An x-ray.
    - Etc.

Component 4/Unit 8c Health IT Workforce Curriculum Version 1.0/Fall 2010 9



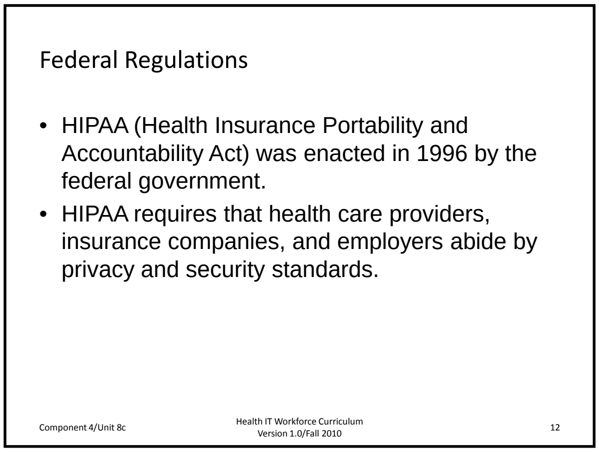
EHRs Used by Health Care Providers

- EHRs are maintained by health care providers.
- EHRs are covered by HIPAA rules.
- EHRs utilize centralized database systems to integrate patient intake, medical care, pharmacy, billing, etc. into one system.
- Departments/entities may not be in same physical location, so patient data must travel over the Internet.
- People can view their own health record, taking ownership of its contents, ensuring accuracy, etc.



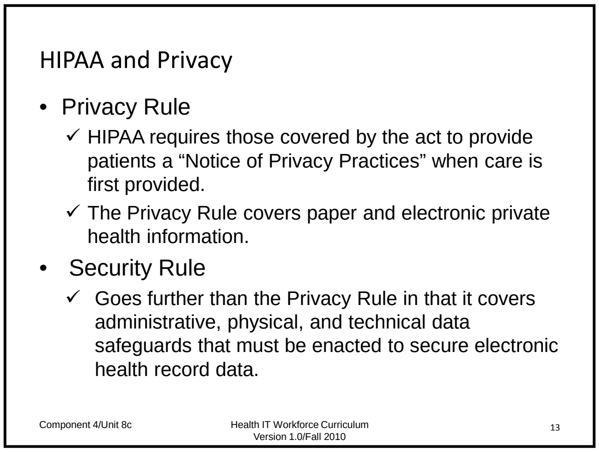
EHR Security Q & A

- How is my data sent over the Internet?
  - ✓ It should be sent in an encrypted, secure manner over the Internet.
- Is my data safe?
  - Much depends on each organization’s physical record and network security practices.
  - No data is 100% secure against theft or misuse.
- Who can view my health records?
  - ✓ Only those who need to know or view the contents of your health record should be able to view it.
  - ✓ You must authorize all other access.



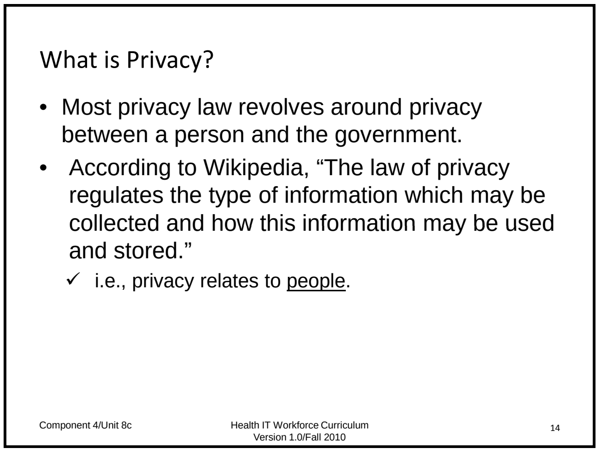
Federal Regulations

- HIPAA (Health Insurance Portability and Accountability Act) was enacted in 1996 by the federal government.
- HIPAA requires that health care providers, insurance companies, and employers abide by privacy and security standards.



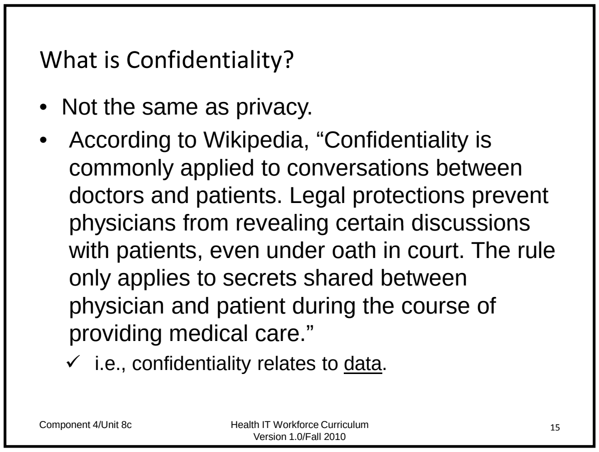
HIPAA and Privacy

- Privacy Rule
  - ✓ HIPAA requires those covered by the act to provide patients a “Notice of Privacy Practices” when care is first provided.
  - ✓ The Privacy Rule covers paper and electronic private health information.
- Security Rule
  - ✓ Goes further than the Privacy Rule in that it covers administrative, physical, and technical data safeguards that must be enacted to secure electronic health record data.



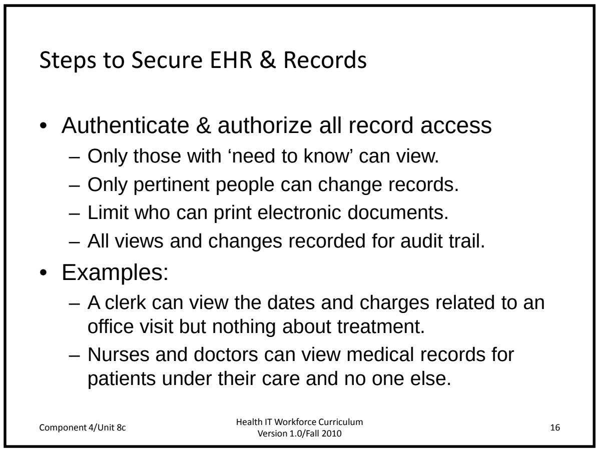
What is Privacy?

- Most privacy law revolves around privacy between a person and the government.
- According to Wikipedia, “The law of privacy regulates the type of information which may be collected and how this information may be used and stored.”
  - ✓ i.e., privacy relates to people.



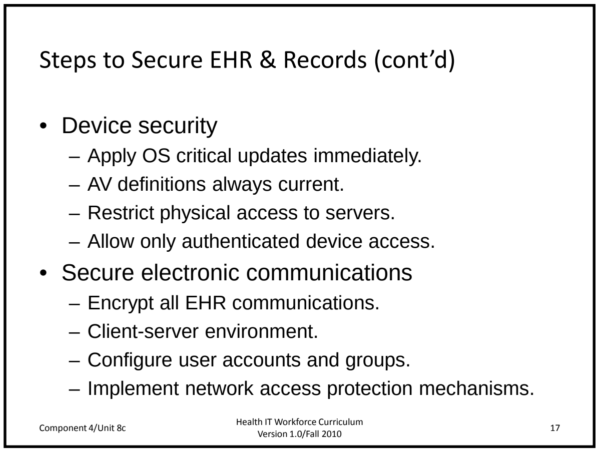
What is Confidentiality?

- Not the same as privacy.
- According to Wikipedia, “Confidentiality is commonly applied to conversations between doctors and patients. Legal protections prevent physicians from revealing certain discussions with patients, even under oath in court. The rule only applies to secrets shared between physician and patient during the course of providing medical care.”
  - ✓ i.e., confidentiality relates to data.



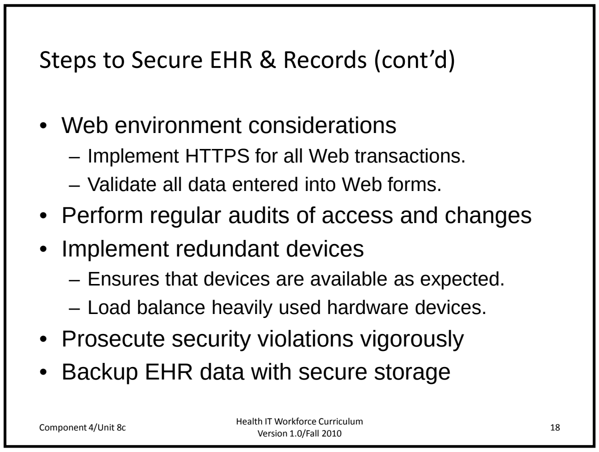
Steps to Secure EHR & Records

- Authenticate & authorize all record access
  - Only those with ‘need to know’ can view.
  - Only pertinent people can change records.
  - Limit who can print electronic documents.
  - All views and changes recorded for audit trail.
- Examples:
  - A clerk can view the dates and charges related to an office visit but nothing about treatment.
  - Nurses and doctors can view medical records for patients under their care and no one else.



Steps to Secure EHR & Records (cont’d)

- Device security
  - Apply OS critical updates immediately.
  - AV definitions always current.
  - Restrict physical access to servers.
  - Allow only authenticated device access.
- Secure electronic communications
  - Encrypt all EHR communications.
  - Client-server environment.
  - Configure user accounts and groups.
  - Implement network access protection mechanisms.



Steps to Secure EHR & Records (cont’d)

- Web environment considerations
  - Implement HTTPS for all Web transactions.
  - Validate all data entered into Web forms.
- Perform regular audits of access and changes
- Implement redundant devices
  - Ensures that devices are available as expected.
  - Load balance heavily used hardware devices.
- Prosecute security violations vigorously
- Backup EHR data with secure storage