

HealthStream Course
Providence Alaska Medical Center
Annual Safety Update 2011

**Integrity, Compliance, Privacy
and Data Security**



To achieve the learning objectives we will:

- Review privacy and security policy changes
- Review new breach notification laws and how they may impact your role.
- Review patient rights

When faced with an integrity, compliance or privacy concern, volunteers should speak with the Volunteer Coordinator, or their supervisor, or call the Integrity Hotline or contact the Privacy Lead.

Providence policy prohibits retaliation against any workforce member who reports a concern in *good faith* or who assists in the investigation of a concern. Good faith reporting is protected under Providence's Non-Retaliation Policy.

There have been significant changes in Privacy and Security regulations and policies this year. We will discuss what's new in:

- Penalties for HIPAA violations (Health Insurance Portability and Accountability Act)
- Reporting privacy and security breaches
- Policies on device and media handling
- Risks to Protected Health Information (PHI) and Social Networking Media

Remember: Patient care includes caring for our patient's protected health information.

Protected Health Information (PHI) and Personally Identifiable Information (PII) are two types of information that require special handling by everyone in health care.

Protected Health Information (PHI) includes but is not limited to:

- **Electronic or paper progress notes**
- **Lab results**
- **X-Ray images**
- **Billing information**
- **Prescription information**
- **Diagnosis**

HIPAA (Health Insurance Portability and Accountability Act) applies to all forms of an individual's protected health information—whether created by a health care provider, health plan, public health authority, life insurer, employer, school, university, or health care clearing house.

HIPAA protects this information whether it is in electronic, written or oral form.

Personally identifiable information or PII, is any information that uniquely identifies an individual, and can include your name and:

- **Social Security Number**
- **Driver's License Number**
- **Account Number**
- **Credit or Debit Account Number**

Depending on your state of residence, other information may also be included as personally identifiable information (PII) under state law. Most states require you to be notified if your personally identifiable information (PII) is compromised.

Why is protecting protected health information (PHI) and personally identifiable information (PII) a special obligation at health care facilities?

Because of the special nature of the information contained at health care facilities and the large number of individuals that have access to that information, health care facilities are at risk for identity theft. Few other businesses hold as much personal, financial and health information about its customers in one place.

The impact of misusing data from a health care facility can be devastating, long-lasting and costly for patients and the facility. In some cases, it can take years for individuals to recover from the impact of a stolen identity.

In 2009 there were two significant developments in privacy that affect health care organizations and their employees:

- Penalties increased significantly for inappropriate use or unauthorized disclosure of protected health information. Employees, and volunteers, as well as companies, can now be fined and face civil or criminal charges for violations.**
- Breaches for violations of HIPAA are now required to be reported**

In April 2010, a former UCLA Healthcare System employee became the first person sentenced to prison for violating the HIPAA Privacy Rule. The employee, a researcher and surgeon, pleaded guilty to snooping in medical files that he had no reason to see. Most of the files belonged to celebrities.

There was no evidence that the researcher accessed the records for profit. It appears he was just curious. His curiosity cost him four months in prison.

Don't let your curiosity get the best of you. Don't peek if you don't have a need to know.

A breach occurs when someone accesses, uses or discloses protected health information (PHI) without authorization and the security or privacy of that information is compromised.

It is important to report a suspected incident even if you are not sure it is a breach so that Providence can properly investigate and do the right thing. If you fail to report a potential privacy or security violation, you could be subject to sanctions up to and including termination.

The rising use of social media like Facebook, MySpace, Blogs and Twitter poses new challenges for health care. As more employees and volunteers use these forms of social media for information exchange, there is an increasing risk that this exchange can include protected health information (PHI) or other types of Providence confidential information.

Providence expects every workforce member to act in accordance with the Code of Conduct, report noncompliance and take an active part in maintaining the integrity and compliance within our ministries.

Creating a professional and ethical workplace is a shared responsibility that involves all Providence leaders, employees and volunteers. Our leaders, managers and supervisors want to hear concerns. When risks are identified early, action can be taken to reduce those risks

Reducing risk means maintaining the reputation of Providence and of its workforce members, the people who deliver care and services to thousands every day.

Patient Rights

Patients have the right to receive a Notice of Our Privacy Practices (NOPP)

Patients have a right to access their own information.

Patients have the right to expect Privacy and Confidentiality.

2011 Volunteer Annual Safety Update (ASU) Test Questions

Please open the 2011 Answer Sheet, print that document and mark your answers on the answer sheet.

Another option would be to open the 2011 Test Questions document, print it and mark your answers, then return either one to Volunteer Services.

Integrity, Compliance, Privacy and Data Security

15. You are aware that a co-worker has inappropriately disclosed private information about one of our patients. It is your responsibility to:

- A. Tell your supervisor
- B. Contact the Privacy Lead
- C. Call the integrity Hotline
- D. Any of the above

16. Protected Health Information (PHI) includes:

- A. Electronic progress notes
- B. Lab results and x-ray images
- C. Billing information
- D. All of the above

17. You see a co-worker in the waiting room of the hospital Emergency Room... You should:

- A. Ask another employee why she is there
- B. Respect your co-worker and allow her to decide if she wishes to initiate conversation
- C. Try to get her to disclose personal information
- D. Look her up in the Admitting records

18. Patient privacy rights include:

- A. The right to receive a Notice of Our Privacy Practices (NOPP)
- B. The right to access their own information
- C. The right to Privacy and Confidentiality
- D. All of the above