FAIRWARNING®

Minimizing Risk
In the Post-HIPAA World

Introduction

- Why are we here?
  - To learn about the FairWarning® automated access auditing program and how it works
  - To sharpen your understanding of your obligations in the handling of confidential health information
  - To acquire the analytical tools to make sound decisions regarding PHI
  - To find out how to avoid inappropriately accessing information that could lead to disciplinary sanctions

Quick Review of HIPAA and PHI

HIPAA Privacy Rule

- **Health Insurance Portability and Accountability Act**
  - Standards for Privacy of Individually Identifiable Health Information
  - The HIPAA Privacy Rule provides federal protections for personal health information.
  - Required reporting for Yale University

PHI

- **Protected Health Information**
  - Any information that identifies an individual or might reasonably be used to identify an individual and relates to:
    - The individual's past, present or future physical or mental health; OR
    - The provision of health care to the individual; OR
    - The past, present or future payment for health care.

What is FairWarning®?

FairWarning® is software that facilitates the monitoring process of access to various ePHI containing systems (EPIC, Synapse, etc.).

Why Audit? and Why Now?

- User access audits are mandated by HIPAA, to protect the privacy of patient information, and to detect any unauthorized access, use or disclosure. Now that we have this technical capability to *automate* the audits, HIPAA requires us to do so.
- Conducting access audits is a way to monitor staff compliance; another HIPAA requirement

- HIPAA program has always conducted access audits both proactively as well as in response to complaints.

How Access Auditing Works

User Name

Mode or Function Used

Patient Name

Time and Date of Access

Audits Enabled by FairWarning®

FairWarning® dramatically increases the efficiency of access auditing, making it possible to increase the amount of audits in the time that it would ordinarily take to do a single audit.

How Will Audit Results Be Handled?

- Each finding will require follow-up to determine if the access was actually inappropriate.
- If an access appears to have been inappropriate (i.e., not ***required or allowed for the performance of your job***), then further follow up will be conducted following standard procedures including:
  - Union notification/representation
  - HR, employee and supervisor input
  - Circumstances of the incident

What is meant by “required for the performance of your job”?

Apply this analytical test…

Ask yourself:

1. Is access to this record or this information part of my daily job requirements?
2. Is this access necessary for Treatment, Payment or Health Care Operations?
3. Am I accessing information to do something that will help a patient in some way, even though it is not part of my regular job?
4. Is there any other way that I can obtain this information other than accessing the account?

If Your Job Requires You To….

- Update a patient's registration
- Follow up on a claim submission
- Document a patient's vital signs
- Change the patient's insurance information and it is someone that you know
- Append an operative note to a claim that has already been submitted

-If the answer is “YES”…

Then YES
Access is required or permitted for work-related purposes

What About Accessing PHI for Personal Use?

- Your co-worker's birthday is coming up but you can't remember the exact date and want to send out a card.
- You need the new address of your ex-spouse to give to your attorney.
- You heard that Joe Starr from your favorite show was seen at Yale. You wonder what he came in for.
- You had the same surgery as a friend of yours in another department and want to compare your charges and operative notes. Your friend gave you permission.
- You are curious to see if your sister's surgery charge got resubmitted with the operative notes yet.

Apply the test……..

Ask yourself…

1. Is access to this record or this information part of my daily job requirements?

2. Is this access necessary for Treatment, Payment or Health Care Operations?

3. Am I accessing information to do something that will help a patient in some way, even though it is not part of my regular job?

4. Is there any other way that I can obtain this information other than accessing the account?

-If the answer is “NO”…

Then Access is most likely prohibited!

When in doubt or unsure, use this rule of thumb…ASK!

REQUIRED

ALLOWED

REQUIRED

ALLOWED

What is meant by “allowed”?

REQUIRED

REQUIRED

ALLOWED

ALLOWED

What Would You Do?

- A patient comes into the office and asks you to help her to find her doctor. She has the doctor's name but not the department.
- A patient calls to ask you for the dates of his last three doctors' appointments, for insurance purposes.
- You found a patient's wallet just outside the entrance to your office. Inside there is an appointment card for an appointment earlier that day. You want to let him know you found it.
- You retrieve a fax marked "RUSH" but it does not indicate to whom it is going. There is a patient name on the fax and no other information. You want to figure out who this "RUSH" fax should be given to.

Apply the test……..

Ask yourself,

1. Is access to this record or this information part of my daily job requirements?

2. Is this access necessary for Treatment, Payment or Health Care Operations?

3. Am I accessing information to do something that will help a patient in some way, even though it is not part of my regular job?

4. Is there any other way that I can obtain this information other than accessing the account?

What Would You Do?...cont

1) It's Friday and you find your co-worker somehow dropped his credit card out of his wallet. He's already left work and is leaving for vacation tomorrow! You don't have his phone number but you think he's been to YMG as a patient when he broke his leg last winter skiing.

2) A newspaper article indicates a young child is missing. You recognize the name in the paper as a name that was on your work-list. You remembered because it was an unusual name you don't usually hear. Should you check to see if the patient was here?

If you are unsure
of the answer to ***any*** question

ASK FOR HELP

before you access that information

Two More HIPAA Terms

Role-Based Access

HIPAA requires us to limit what users can and cannot do and see. This means assigning user privileges based on job duties and workflows.

Adjustments in privileges – large and small – are to be expected.

Meanwhile, be aware that you might be able to do and see more than you need to.

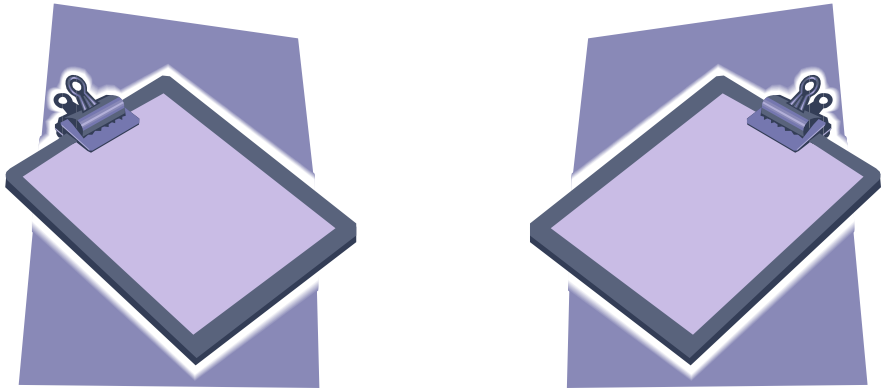
Minimum Necessary (MN)

HIPAA requires us to access only the information that we need in order to perform our duties; patient billing and certain practice management functions.

Self Assessment

What DID NOT Change with FairWarning®

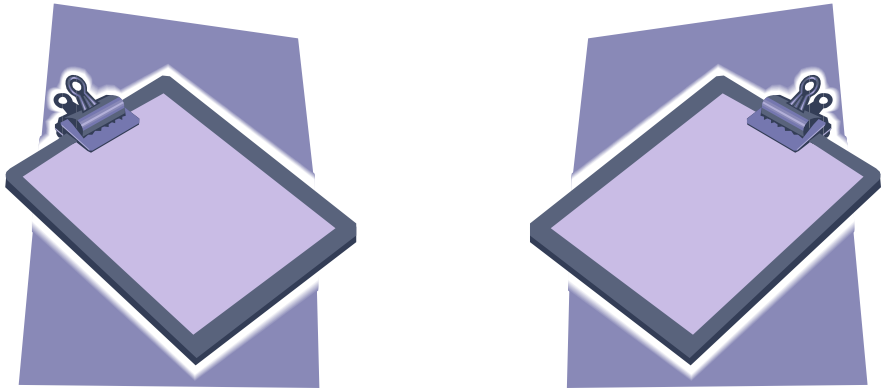
- Your job duties did not change
- Rules for when you can and cannot access PHI did not change



What Did Change with FairWarning®

Implementation of FairWarning® Audits Dramatically Change the Likelihood of Discovering Unauthorized Access . . .

In Real Time



THE GOAL IS TO HAVE ZERO INSTANCES OF INAPPROPRIATE ACCESS

Best Practices to Minimize Risk

1. Do not mistake the EMR for a telephone directory.
2. Because you can…does not mean you should.
3. **NEVER** write down or share your passwords.
4. If you access a record or screen by mistake, exit out immediately, tell your supervisor, and continue with your work.
5. Log out of your computer or lock your computer when you walk away from it.
6. Do not let the fear of an "audit hit" hinder your job performance.
7. If in doubt…**ASK**!

Resources

- Your Supervisor
- HIPAA Privacy Office

hipaa@yale.edu

203-432-5919

- www.yale.edu/hipaa

Q&A

Analytical test…

Ask yourself…

1. Is access to this record or this information part of my daily job requirements?
2. Is this access necessary for Treatment, Payment or Health Care Operations?
3. Am I accessing information to do something that will help a patient in some way, even though it is not part of my regular job?
   - *Promote patient safety? Prevent missed appointment? Improve patient experience? Provide good customer service? Promote efficiency in our workflow?
4. Is there any other way that I can obtain this information other than accessing the account?