UCONN HEALTH
OFFICE OF HEALTHCARE COMPLIANCE & PRIVACY

Protecting Patient Privacy with FairWarning Frequently Asked Questions

What is FairWarning?

FairWarning is a privacy monitoring technology that interfaces with EPIC and axiUm and analyzes user activity to detect potentially inappropriate access to patient information and other privacy violations. For example, FairWarning helps detect user activities including, but not limited to:

- Inappropriate access to patient records, including:
  - User "snooping," such as when an employee accesses a coworker's medical or dental record out of curiosity and without a job-related need to know;
  - Inappropriate user access to a high profile patient's medical record (e.g., celebrity, person of interest in the news, or UConn Health manager/senior leader);
- Multiple failed log-in attempts by a single user (indicating, for example, potential compromise of the user's credentials);
- Unusual or atypical activity, such as unusual amounts of printing or activity that is outside of a user's normal workflow.

How does FairWarning work?

FairWarning analyzes EPIC and axiUm user activity and flags instances of potentially inappropriate activity. If potentially inappropriate activity is detected, the user's manager is notified. This is similar to the UConn Health Office of Healthcare Compliance and Privacy's (OHCP) longstanding practice of notifying a user's manager upon receiving a report of potentially inappropriate user activity. The responsible manager reviews the activity in question and determines whether it was appropriate. The privacy team investigates further on an as-needed basis.

Doesn't the Privacy Office already receive and respond to reports of inappropriate user activity?

Yes, the privacy team already receives and responds to reports of potential unauthorized user activity, typically from individual employees or others who bring these concerns forward. FairWarning is an additional way for UConn Health to monitor for inappropriate activity. Employees should continue to report concerns to the privacy team (or to a supervisor, who must then report the concern to OHCP). FairWarning supplements these reports and thus enhances UConn Health's ability to protect patient privacy.

Please report any privacy concerns to the privacy team via email at privacyoffice@uchc.edu.

What happens if FairWarning flags my user activity as potentially inappropriate?

The privacy team responds to information from FairWarning just as it responds to other reports of potentially unauthorized user activity:

- The responsible manager is notified and reviews the matter to determine whether the activity in question was appropriate.
- If the activity was appropriate, no further action is taken.
- When the activity does *not* appear to be appropriate, or the manager cannot determine whether the activity was appropriate, the privacy team conducts a review and works with management and Human Resources to develop an appropriate response based on the particular circumstances.

What happens if inappropriate user activity is confirmed?

Employees who violate UConn Health privacy or information security policies are subject to sanctions, determined on a case-by-case basis depending on:

- The severity of the violation;
- Whether the violation was intentional or unintentional;
- Whether the violation indicates a pattern or practice of improper use or disclosure of confidential information; and/or
- Other relevant considerations.

If you have questions about FairWarning, please email privacyoffice@uchc.edu .

Relevant Policies:

- 2003-21: Minimum Necessary Data (Privacy and Security of PHI).pdf
- 2014-04: Sanctions Policy for Privacy and Security Violations for Faculty and Staff.pdf