# How to Respond to a Visual Privacy Breach in Healthcare

By Kate Borten, CISSP, CISM

The topic of privacy and security incidents is sometimes confusing to Health Insurance Portability and Accountability Act (HIPAA) Covered Entities (CEs) and their Business Associates (BAs). Incidents can fall anywhere on a continuum of risk from an event such as an incidental disclosure of Protected Health Information (PHI) to a breach with a significant risk of harm to patients.

It is important for CEs and BAs to have an extensive, detailed incident response plan to follow whenever a visual privacy incident is reported. Such a plan will help an organization quickly determine whether the event is:

(a) an incidental disclosure;

(b) an incident that violates security and/or privacy policy and HIPAA; or

(c) a violation that is also a breach posing a potential risk of patient harm.

These distinctions are important to an organization because they will determine how to respond to each individual event. If the incident is a breach, according to definitions in certain state laws and the Health Information Technology for Economic and Clinical Health (HITECH) Act, then very specific steps must be taken within a strict timeframe.

In the following examples you'll learn three different ways how PHI can be exposed on computer screens, each demonstrating a different level of risk and organization response.

## An incidental disclosure of PHI

**Incident:** As an alternative to the traditional front desk check-in process, a medical practice installs a kiosk in the waiting room where patients are encouraged to check themselves in at a computer. The information displayed onscreen is limited to demographic data (such as name, address, and telephone) and insurance information; there is no clinical data displayed. In spite of these precautions, another patient or visitor can walk up alongside or behind the patient checking in and read the screen.

**Response:** If the medical practice installs a privacy filter on the kiosk, the scenario above would be considered an "incidental disclosure" of PHI, and it is not a violation of HIPAA's privacy rule since reasonable security measures have been taken and the risk of harm is low. It is comparable to one patient overhearing another patient's conversation at the front desk or recognizing another patient in the waiting area.

## A PHI disclosure that is a violation but not a breach

**Incident:** A hospital volunteer sits at a desk in a prominent spot in the lobby, ready to help visitors find a particular patient they're there to see. The volunteer has limited computer system access and can only view a patient list showing patient location and

### Penalties and Enforcement

The HITECH Act, a subset of the 2009 American Recovery and Reinvestment Act, expanded the civil monetary penalties for non-compliance with HIPAA privacy and security regulations. There are now four tiers with increasing penalties depending on factors such as willful neglect. However, any violation, regardless of the tier, can result in a penalty of $1.5 million for multiple occurrences of the same violation within a calendar year. There is no overall cap on non-compliance penalties, and a complaint can lead to a full audit that may uncover a multitude of vulnerabilities.

Adding to these expanded fines, the HITECH Act requires the U.S. Department of Health and Human Services (HHS) to perform audits of Covered Entities and their Business Associates, and the Act authorizes state attorneys general to bring action when state residents have HIPAA privacy complaints. In response, HHS is providing state AG training, and in June 2011 HHS awarded over $9 million to KPMG to perform 150 privacy and security audits by the end of 2012.

Congress and HHS take violations very seriously. They intend for the healthcare industry to pay attention to patient privacy and security.

general status. The volunteer has been reminded to log off before leaving his desk. But one evening he is rushing to leave and forgets to log off. Neither the computer nor the application has an automatic inactivity timeout feature. However, another worker notices and promptly logs the volunteer off.

**Response:** The volunteer's failure to log off should be treated as a violation of the hospital's policy and procedures. And the lack of an automated safety net is a violation of HIPAA's security rule. This scenario constitutes a HIPAA violation, and the hospital should document it and follow up with sanctions and mitigation. To reduce the risk of a recurrence, workers should receive additional reminders, a technical safety net (an auto logoff or the equivalent alternative) should be implemented, and a privacy filter should be installed on the computer.

But this violation does not rise to the level of a breach because the exposed PHI in the facility directory is limited in nature and the failure to log off was caught before a visual hacker could take advantage of the information displayed.

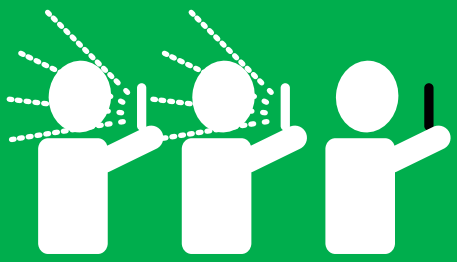
## A PHI disclosure that is a violation and a breach

**Incident:** An oncologist routinely reviews his cases and types notes on his laptop while he commutes to and from his office. It's an hour-long train ride, so this is valuable work time. However, the train is usually full and he does not use a privacy filter on his laptop. That means his patients' names and clinical details are displayed in clear view of the passengers on either side, offering an easy chance of visual hacking.

**Response:** This is a violation of both HIPAA's privacy rule and the security rule. While the PHI disclosures are unintentional, such disclosures of PHI to the general public are unnecessary, inappropriate, and unauthorized, and security measures to prevent such ongoing disclosures are absent. A privacy filter should be used, and the doctor should try his best to position himself so that other commuters will not have access to the data displayed on screen. He should only review his cases on the train if he is properly positioned and using the correct safeguards in order to reduce exposure of confidential patient information to visual hackers.

Further, since this is sensitive and detailed PHI, it has the potential for significant harm to each of his patients. Therefore, this violation rises to the level of a breach requiring notification to affected patients and HHS.

To limit the potential harm to patients and the affected organization, CEs and BAs need to make sure their detailed incident response plans allow them to quickly and thoroughly respond to a visual privacy incident. But it is even more important to take steps to prevent incidents and breaches from happening in the first place. When it comes to visual privacy, CEs and BAs should have clear policies, thorough workforce training and reminders, and the physical security protection of privacy filters wherever appropriate.

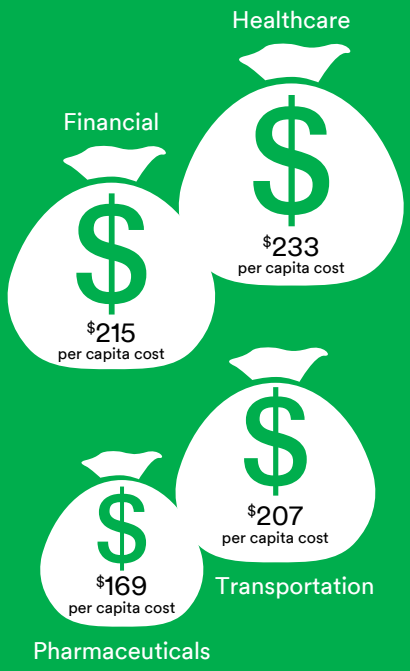


## 2/3

Number of working professionals who display sensitive information on their mobile devices when outside the office[1]

## Top 4

high cost of data breaches[2]




**3Mscreens.com**

[1]"Visual Data Breach Risk Assessment Study," People Security, commissioned by 3M, 2010.
[2]"2013 Cost of a Data Breach Study: Global Analysis," Ponemon Institute/Symantec.



**Privacy is the best policy.** | 3M