eALERT

INCompliance

August 6, 2012

Don't Let This Be You:
Safeguard Your Multimedia Protected Health Information

The Scenario. Your hospital's bariatric clinic regularly takes "before and after" photos of patients to chronicle the results of their weight-loss surgeries. One morning, you receive a frantic phone call: "Is this the Privacy Officer? I think we have a problem. A digital camera filled with photos of bariatric clinic patients was stolen last night."

The Investigation. You realize that the theft of this camera could constitute a reportable breach of protected health information (PHI). You immediately launch an investigation to obtain facts that will allow you to review and assess whether the incident actually qualifies as a reportable breach.

Your investigation reveals that the bariatric clinic takes a photo of each patient before and after weight-loss surgery. The patients are photographed from head to toe, and they are entirely unclothed. The bariatric clinic staff believes that the camera's memory card contains photos taken during the past eight months, but they cannot pinpoint the date when the card was first used. Their best estimate of the number of patients whose photos are on the stolen memory card is 650. Anyone in possession of the camera could view, print, copy, and distribute the photos contained on the memory card.

The bariatric clinic did not have any policy or procedure in place regarding the camera. At the end of each day, the camera was left on top of a desk in a patient room. The clinic did not have any procedure in place regarding when the memory card was to be erased or when the photos were to be transferred to the patients' electronic medical records. When a memory card became full, the staff member using the camera would simply remove the memory card, place it in a desk drawer, and insert a new card.

The Assessment. With your investigation complete, you begin your assessment of whether this incident constitutes a reportable breach. First, you must determine whether PHI was involved. There might be some tendency to think that PHI was not involved in this incident, as there were no paper or electronic textual records involved. However, in addition to such data elements as names and addresses, the HIPAA Privacy Rule also includes "full face photographic images and comparable images" in its list of identifiers that must be removed in order to "de-identify" PHI. The photos on the camera's memory card included the patients' faces, and this incident therefore involved PHI.

Moving on to the next step in the assessment, you consider whether the PHI was unsecured. The only methods of securing PHI are encryption and destruction. The camera's memory card was not encrypted, and it was obviously not destroyed. The PHI was therefore unsecured.

The third and fourth steps of the assessment require you to analyze whether the incident was a breach, and if so, whether there was an unauthorized access, use, or disclosure of PHI. Breach is defined as the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rules which compromises the security or privacy of the PHI. A breach only occurs if there is an unauthorized

acquisition, access, use, or disclosure of the unsecured PHI. There must be a violation of the HIPAA Privacy Rule for there to be a breach. A theft of PHI is an acquisition or disclosure of PHI that is not permitted by the Privacy Rule. The theft of this camera was accordingly a breach, and there was certainly an unauthorized acquisition or disclosure of PHI in violation of the Privacy Rule.

Arriving at the fifth and final step in the assessment, you consider whether the breach compromised the security or privacy of the PHI involved. You must analyze whether the breach poses a significant risk of financial, reputational, or other harm to the patients whose PHI was stolen. Because this incident involved a theft, the individual in possession of the PHI cannot be expected to maintain the confidentiality of the information, and his motives are certainly suspect. The types of information disclosed were some of the most personal and sensitive in the possession of any covered entity. There is no way to prevent the thief from further disclosing the photos to others. Based upon all of these facts, it must be concluded that this breach does pose a significant risk of harm to the patients whose photos are on the camera's memory card.

The Response. Once you have concluded that this was a reportable breach, you must now work with the bariatric clinic to notify the patients involved. Given the uncertainty as to when the memory card was first used, this will be a difficult task. Further, because this breach involved more than five hundred individuals, you must also promptly notify local media and the U.S. Department of Health and Human Services.

Beyond the significant task of providing these notices, your organization must also implement new procedures and safeguards to prevent this type of breach from occurring again. You must also be prepared to respond to an investigation by the HHS Office for Civil Rights and to pay any fines that might be levied as a result of the investigation.

The Lessons. A reportable breach of PHI does not always involve textual records. More and more, providers utilize photos and videos in a wide array of clinical settings. We recommend that HIPAA Privacy Officers compile lists of every camera and video camera utilized in their organizations. This is the first step to implementing policies and procedures that will prevent the type of breach described above.

The policies should direct staff to include patients' faces in photos or videos only when absolutely necessary. If the memory card in this scenario had contained photos that did not include the patients' faces, the photos would likely not have constituted PHI, and there would not have been a breach.

Second, there should be standard procedures for the erasure or transfer of photos or videos from the devices to patients' medical records or other appropriate locations. If the photos or videos are considered part of the medical record, they ultimately belong in the record, not on a memory card. Had the memory card in this scenario been erased at regular intervals, it is unlikely that the covered entity would have had to report a breach affecting more than five hundred individuals to HHS and the media.

Finally, we recommend that any device containing photos or video that constitute PHI be stored in a secure location. This is a reasonable safeguard that should not be an undue expense for any covered entity. Had the camera in this scenario been locked in a secure drawer in the bariatric clinic, it would not have been stolen, and this covered entity would not have had a breach to report.

The time spent implementing these recommendations is minimal when compared to the time and expense of investigating a breach, making the required notifications, and implementing appropriate changes in response to the breach.

Does your organization adequately protect its photos and videos? The consultants of INCompliance will conduct a thorough HIPAA audit of your organization, and we will work with you to correct any deficiencies *before* you have a breach.

This eAlert was prepared by Chris Bennington (513) 870-6572 or cbennington@incomplianceconsulting.com.
Please contact any INCompliance consultant for more information at info@incomplianceconsulting.com .