# The Impermissibles!

No; this is not a novel about tommy gun wielding gangsters being chased down by heroic police and detectives. Instead, it is a short story about impermissible disclosures. You see, individuals often use the term "breach" instead of using the proper verbiage to describe an incident or event that may lead to a breach. Breach seems to have become the fall back word for anything that may violate the HIPAA rule. Additionally, staff often do not understand what are the precursors to a breach, or what the indicators are. Having a sound understanding of what an impermissible is and is not, will help your staff identify an incident, respond to the incident, and hopefully avoid a breach or respond to a potential breach.

We begin by identifying the four types of impermissibles; they are ***access, acquisition, use,*** and ***disclosure***. Each of these four impermissibles represent incidents or events where PHI was seen or obtained by someone without proper authorization, whether inside or outside your organization.

***Access*** means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. However, when someone who is not authorized to access the data, and does so, the event is known as an impermissible access. For example, a user's access into an EMR is unrelated to his/her duties such as when a receptionist looks through a patient's records to learn what treatment was provided and has no official reason for doing so, or a technician inappropriately accesses a neighbor's PHI out of curiosity to confirm a rumor, or a lab technician attempts to view sensitive medical data not related to laboratory diagnostics such as behavioral health records. These events are referred to as impermissible access.

***Acquisition*** is the "act of obtaining" something and for this story, that something is PHI. You may acquire PHI as part of your duties since you are authorized to do so, however, when you are not an authorized employee and you acquire the PHI, we refer to this event as an impermissible acquisition. The following examples will help you understand this type of impermissible; a briefcase containing patient medical documents is stolen from your office, or an unencrypted laptop is stolen from your backpack left in your car, or lastly, an unencrypted flash drive containing patient's names, SSN, and diagnosis is removed from your hotel room. These events constitute an impermissible acquisition. Note that in each example, the acquisition took place outside of the organization though that is not always the case.

***Use*** means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within the entity that maintains such information. In other words, use of PHI takes place inside your organization, not outside of it. Again, you can use PHI for official business, however, when your use extends beyond official business, or extends beyond what is needed to do your job, (minimum necessary), we refer to the event as an impermissible use. For example, a member of your quality assurance committee examines additional medical information that is not required for the quality review, or a technician obtains more than the minimum necessary PHI on a patient to provide medical care, & finally, the ER nurse provides extra interesting medical information to the registration clerk which is not needed to register the patient into the facility. These events constitute an impermissible use of PHI.

***Disclosure*** means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information. When you disclose PHI, you must ensure you are disclosing only to those who are authorized to receive the PHI. Examples of impermissible disclosures include PHI mistakenly faxed to a grocery store instead of another physician's office, EOB or Explanation of Benefits mailed to the wrong patient, posting a patient's HIV status on a personal Facebook account, or lastly, sending an e-mail containing PHI to wrong patient. These incidents are called impermissible disclosures.

In summary, events where unauthorized individuals access, acquire, use, or disclose PHI are known as impermissibles. It is important that your staff understand these impermissibles because they are the precursors to a breach. To understand this relationship, the breach rule reads that a breach means "any *acquisition*, *access*, *use*, or *disclosure* of PHI in a manner not permitted under the privacy rule, which compromises the security or privacy of the PHI". In other words, any unauthorized *access*, *acquisition*, *use*, or *disclosure* is considered a breach and you must conduct an investigation to prove otherwise. In some cases, the incident constitutes a disclosure and acquisition, or a use and disclosure, so combinations of the categories are possible. It stands to reason, your staff needs to have a good understanding of these four categories of impermissibles, and therefore, it would be prudent to consider telling the story of the "Impermissibles" at your next training session.

**Hernan Serrano Jr.**
www.HIPAAtrek.com
hernan@hipaatrek.com

# The Impermissibles!

| | |
|---|---|
| Medical record documents left in cafeteria used by the public. | Disclosure |
| User inappropriately accesses family members' PHI | Access, Use |
| PHI mistakenly faxed to a grocery store (ex. prescription, test results). | Disclosure |
| Stolen/lost laptop containing unsecured PHI. | Acquired, Disclosure |
| PHI mistakenly faxed to an incorrect pharmacy (covered entity). | Disclosure |
| Lab results sent to incorrect provider at non-[org] facility. | Disclosure |
| Paperwork for two other patients provided to patient. | Disclosure, Acquired |
| Test results faxed to provider's former organization. | Disclosure |
| Lab results sent to incorrect provider at [org] facility & is not further used or disclosed. | Use |
| EOB (Explanation of Benefits) sent to wrong guarantor. | Disclosure |
| A patient's discharge paperwork is left lying in patient's room & found by someone other than that patient or staff member. | Disclosure, Acquired |
| Claim sent to known terminated insurance company. | Disclosure |
| Surgical order sent to incorrect healthcare facility. | Disclosure |
| EMT takes a cell phone picture of patient following a MVA and transmits photo to friends or posts on Facebook. | Disclosure, Use |
| Medical record copies in response to a payer's request was sent to an incorrect payer, lost in mailing process, and never received or returned. | Disclosure, Acquired |
| Info given to a family member without a password (for a patient who requested restricted access). | Disclosure |
| Provider verbally informed adult patient's mother of test results. | Disclosure |
| Incorrect patient's immunization sent to a parent. | Disclosure |
| Scheduler informed a patient of another patient's name who was treated for mental health, HIV, STDs, etc. | Disclosure |
| Patient's name and type of services announced in a patient waiting area - other patients present. | Disclosure |
| Briefcase containing patient medical record documents stolen. | Acquired, Disclosed |
| Transcription documents improperly disposed of at an employee's residence. | Disclosed |
| Papers containing PHI found scattered along roadside after improper storage in truck by business associate responsible for disposal (shredding). | Disclosed |
| User inappropriately accesses neighbors' PHI. | Access, Use |
| User inappropriately accesses celebrity's' PHI. | Access, Use |
| Unencrypted flash drive lost that contains database of patients participating in a clinical study. | Acquired, Disclosed |
| User access is unrelated to his/her duties (ex. A receptionist looked through a patient's records to learn what treatment was provided). | Access, Use |
| Misdirected e-mail of listing of drug seeking patients to an external group list. | Disclosed |