HIPAA Violations

Laura Asbell, PhD

Compiled on September 10, 2017

Following is a list of HIPAA complaints and violations by category, with examples. On the HIPAA site, categories of violations, examples, and frequencies are listed for all violations. Most of the violations and examples apply to large organizations and would not be relevant for a psychologist, even as an employee of one of these organizations. The categories and examples below are from their data or extrapolated from their data. They are not in order of likelihood of relevance specifically to a psychologist. They are listed by the top five categories of complaints per year, and the top five violation categories change depending on the year, probably as organizations become better trained and experienced. In 2015, there were 17,694 resolved complaints, with 1089 of those investigated and 730 of those (67%) requiring corrective action. This number was down from a high of 4464 investigations with 3470 requiring corrective actions in 2013.

1. Impermissible Uses and Disclosures
    a. A staff member or employee accessed PHI for personal curiosity.
    b. Disclosure to law enforcement made without law mandating disclosure.
2. Safeguards
    a. Provider discussed issue with a client in the waiting room
    b. Provider's computer screen with PHI was visible to another client.
    c. Not having used a fax cover sheet underscoring it was a confidential communication for an intended recipient.
3. Access
    a. Not giving a client access to their records, supplying a summary only or allowing the client to read the records but not get a copy.
    b. Not giving a client access based on non-payment.
    c. Not giving a client access based on a third party payment source, eg, a disability determination evaluation.
    d. Not giving client access to all records, regardless of source. Example given was withholding records from another provider in the patient's record.
    e. Not providing a client the opportunity to having a denial for records reviewed after a denial based on the likelihood it would cause the client substantial harm.
4. Technical Safeguards
    a. Computer or USB device lost with unencrypted PHI.
    b. Cell phone lost without password protection.
    c. Using unencrypted internet transmission of PHI. (Unencrypted communication with a client via email is allowed with specific safeguards. See: www.hhs.gov/hipaa/for-professionals/faq/570/does-hipaa-permit-health-care-providers-to-use-email-to-discuss-health-issues-with-patients/index.html)
5. Minimum Necessary

    a. An entire record sent when a partial record was requested.
    b. Message left for a client on a home phone with more detail than necessary.
6. Complaints
    a. No definition or examples were given on this issue.
7. Notice of Privacy Practices
    a. Notice not given or not acknowledged in writing prior to services.
    b. Provider making privacy rule compliance conditional on the client not airing commentary about the providers' services.
8. Authorization
    a. A provider left PHI on a client's home phone when the client has requested work phone contact only.
    b. A provider accidentally faxed PHI to the wrong entity.
9. Business Associates
    a. Lack of a business associates agreement with an entity given access to PHI. Entity examples might include cloud storage, IT providers, bookkeepers, billing companies, billing programs, CPA firm, law firm, online fax service, and internet video chat vendor.
10. Policies and Procedures
    a. Policies and Procedures addressing HIPAA not in place.
    b. Not notifying HIPAA of a breach.

Excellent reference on HIPAA: https://www.hhs.gov/hipaa/for-professionals/index.html