# HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA): FACT SHEET FOR NEUROPSYCHOLOGISTS

*Division 40, American Psychological Association*

## DISCLAIMER

*This general information fact sheet is made available by Division 40 of the American Psychological Association to outline the requirements of HIPAA regulations that may be of special interest to neuropsychologists. The information is not exhaustive or definitive, nor considered to be guidelines or standards of practice. It has not been endorsed or approved by APA.. One should consult State Laws and the American Psychological Association Principles of Psychologists and Code of Conduct (2003) regarding additional specifics of compliance as the fact sheet does not integrate ethical requirements or non-preempted state laws. The fact sheet may not be applicable to every situation, and is not intended to provide legal advice. Neuropsychologists should seek appropriate legal advice when necessary. The fact sheet is based on an understanding of current information, but the administrative and legal process may result in new information concerning its requirements due to the new and evolving nature of HIPAA. More detailed information, including state-specific information can be obtained through the APA Practice Directorate's course, HIPAA for Psychologists, that can be accessed at their website listed below. Additional resources include the United States Office of Civil Rights, the Centers for Medicare and Medicaid Services, and the Department of Health and Human Services for more specific information. This fact sheet has not been endorsed or approved by these agencies.*

## *General Information*

### What is HIPAA?

HIPAA is the Health Insurance Portability and Accountability Act of 1996. It is a statute and set of Federal rules governing the use and disclosure of health information. The rules involve four components: Privacy Rule (effective 4/14/03), Electronic Transaction Standards and Code Sets (effective 10/16/03), Security Rule (effective 2/21/05), and Employer Identifier Standards (effective August 1, 2005). HIPAA also establishes criminal and civil penalties for improper use and disclosure.

### Is HIPAA relevant to Neuropsychologists?

Neuropsychologists may be required to follow HIPAA regulations in their clinical and research practice, whether they are in private practice or employed by an agency (e.g., Medical School, University, Mental Health Center, or Hospital). Any neuropsychologist who is a covered entity had to be compliant with the Privacy Rule by April 14, 2003. Not everyone will meet the definition of a covered entity. According to HIPAA, covered entities include but are not limited to Healthcare Providers, Health Care Plans, and Healthcare Clearinghouses. A neuropsychologist would become a covered entity if he or she is a healthcare provider who: 1) furnishes, bills, or receives payment for healthcare; 2) conducts one of the 8 covered transactions (such as checking billing claims status, checking authorization for payment, etc.); and 3) conducts any of those 8 transactions electronically (for example via computer, internet, transfer of disks, CDs). If someone does not meet all three of these criteria, then they are not a covered entity and the HIPAA Privacy Rule does not apply to them. However, they may have to interact with other covered entities and therefore it mught be advisable to be aware of the Privacy Rule to properly provide treatment to clients while protecting their health information. If a neuropsychologist engages exclusively in forensic private practice in which no electronic transmission of client information is conducted, then that neuropsychologist would not be a covered entity.

**What is the difference between the Privacy Rule and Security Rule?**

The Privacy Rule focuses on the application of effective policies, procedures, and business service agreements to control the access to and use of patient information. The Security Rule addresses the provider/organization's physical infrastructure to assure secure and private communication and maintenance of confidential patient information. The Privacy Rule applies to all protected health information regardless of the medium in which it is kept and also includes security requirements. The Security Rule applies only to protected health information stored electronically.

**How will the HIPAA Privacy Rule affect neuropsychologists?**

HIPAA generally requires that neuropsychologists provide information to patients about their privacy rights and how that information can be used. One way to meet this requirement is to adopt clear privacy policies and procedures, train employees and supervisees so that they understand privacy procedures, designate an individual responsible for addressing HIPAA privacy questions and complaints, and secure patient records (e.g., test reports, raw data, clinical interview notes). The policies and procedures must be documented in either written or electronic form. HIPAA requires that the neuropsychologist also mitigate any known harmful effects in the unauthorized use or disclosure of patient health information. In addition, the Privacy Rule establishes the conditions under which Protected Health Information (PHI) may be used or disclosed by covered entities for research purposes. PHI consists of information in the records that could identify the patient. Please refer to the glossary for a more detailed definition of PHI.

**How will the Security Rule affect neuropsychologists?**

The Final Rule adopting HIPAA standards for the security of electronic health information was published in the Federal Register on February 20, 2003. This final rule specifies a series of administrative, technical, and physical security procedures for covered entities to use to assure the confidentiality of electronic protected health information. The standards are delineated into either required or addressable implementation specifications. HIPAA requires that neuropsychologists develop clear written policies and procedures to establish physical safeguards to guard data integrity, confidentiality, and availability; employ technical security services to guard data integrity, confidentiality, and availability; and establish technical security mechanisms to guard against unauthorized access to data that is transmitted over a communications network. HIPAA also indicates that neuropsychologists are given some discretion in deciding the feasibility of implementations beyond those that will be required.

**Do the patient rights of the Privacy Rule apply to neuropsychologists too?**

The HIPAA Privacy Rule may grant the client (or their personal representative) a broader access than prior to HIPAA depending on state law. Only under a few well defined circumstances can the healthcare provider deny this request for access and even then in some of these cases, the denial can be reviewable by a third party. One unreviewable reason for denial is a request for the client to review their "psychotherapy notes" as defined by HIPAA However, test reports and raw test data do not fall under the provisions pertaining to "psychotherapy notes." Additionally, individuals may request restrictions as to how a covered entity will use and disclose PHI about them for treatment, payment, and health care operations (one doesn't have to agree to these restrictions but must comply with any agreements made). Individuals may also request to receive confidential communications from a covered entity, either at alternative locations or by alternative means. Finally, any use or disclosure of PHI must be consistent with the covered entities' practices, and the covered entity is required to provide the individual with adequate notice of its privacy practices and a list (called an accounting) of disclosures of PHI.

**What is an accounting under HIPAA?**

The Privacy Rule gives individuals the right to request an accounting of certain disclosures of PHI made by a covered entity. This accounting must include disclosures of PHI that occurred during the six years prior to the individual's request or the compliance date (whichever is sooner), and must include specified information regarding each disclosure. A more general accounting is permitted for subsequent multiple disclosures to the same person or entity for a single purpose. Disclosures made pursuant to an individual authorization or disclosures of a limited data set under a data use agreement are exempt from this accounting requirement. Additionally, for disclosures of PHI without individual authorization that involve at least 50 records, the Privacy Rule allows for a simplified accounting procedure. Under the simplified procedures, a covered entity may provide individuals with a list of all protocols for which the patient's PHI may have been disclosed.

**Are there consequences for failure to comply?**
Yes, there are posted fines and penalties (some substantial) for failure to comply with HIPAA rules. There are scaleable penalties, with consideration for reasonable effort.

***Clinical Information***

**Do patients have access to and can they obtain a copy of their neuropsychological reports?**
Under HIPAA regulations, patients generally now have access to their records, including neuropsychological reports, test responses, and raw data. This is regardless of the referral party (e.g., IME, Worker's Compensation) or reason for referral. (What about if the referral is for litigation purposes?) However, there are some limited defined instances for denying such access within the HIPAA Privacy Rule, and there may be additional guidance from applicable state laws and the American Psychological Association Principles of Psychologists and Code of Conduct (2003). In general, when HIPAA rules are in conflict with other applicable rules, laws, standards, statutes, etc., the more stringent rule (with regard to safeguarding PHI) takes precedence.

**Does HIPAA require patient authorization to send a neuropsychological report to another provider who is treating the patient?**
No, the HIPAA Privacy Rule permits the neuropsychologist to disclose PHI about an individual without the individual's authorization to another provider for treatment of the individual. However, agency or organizational policies (e.g., hospital, mental health center, or university) or state laws that are more stringent regarding the release of information should be followed. If their policies require patient consent, consent must be obtained.

**Are parents allowed access to their minor child's neuropsychological reports?**
Yes, HIPAA generally allows a parent to have access to the records concerning his or her child as the minor child's personal representative when such access is not inconsistent with state or other applicable laws. However, there are three circumstances under the HIPAA Privacy Rule in which the parent is not considered to be the personal representative of a minor child: (1) the minor has consented to care and the consent of the parent is not required by state or other applicable law; (2) the minor has obtained the testing at the direction of the court or an appointee of the court; or (3) the parent of the minor has agreed that the neuropsychologist and the child may have a confidential relationship. In addition, HIPAA allows a neuropsychologist (or provider) to choose not to treat a parent as a personal representative in the case of suspected abuse, neglect, domestic violence, or endangerment to the child.

**Are e-mail correspondences with patients or referral parties covered under HIPAA?**

All electronic transmission of health information by covered entities is covered under HIPAA. Electronic transmission is not necessarily considered a confidential means for use and disclosure of patient information, including electronic transmission with patients themselves, without the consideration of the use of encryption or other security measures. HIPAA requires neuropsychologists to take special care in mitigating any harmful effects and limitations of confidentiality with electronic transmission.

**What is the difference between authorization and consent under HIPAA?**

Prior to using PHI to carry out treatment, payment, and health care operations health care providers under HIPAA are not required but may choose to obtain consent although many states may have a consent requirement. Consent is a general document that gives health care providers permission to use and disclose all PHI for treatment, payment, and health care operations. It gives permission only to that provider, not to any other person. Health care providers may condition the provision of treatment on the individual providing this consent. One consent may cover all uses and disclosures by that provider, indefinitely. Consent need not specify the particular information to be used or disclosed, nor the recipients of disclosed information. Generally, a "direct treatment provider" is one that treats a patient directly, rather than based on the orders of another provider, and/or provides health care services or test results directly to patients. Other health care providers, health plans, and health care clearinghouses may use or disclose information for treatment, payment, and healthcare operations without consent, or may choose to obtain consent. However, many states may have a consent requirement.

An authorization is permission above and beyond the general consent that permits further use for specified purposes. It is required by the Privacy Rule for use and disclosure of PHI for marketing or research, for disclosure of psychotherapy notes, and for any other uses/disclosures that are not for treatment, payment or healthcare operations.

**Is informed consent for testing the same as HIPAA consent?**

No. Informed consent for testing and any consent obtained under HIPAA for treatment, payment, and health care operations are not the same. Although the final Privacy Rule allows for these two types of consents to be obtained in the same document, the two consents must be visually separate. In addition, the privacy notice must be a separate document. Informed consent regarding testing, treatment, or any other procedures still must be obtained from patients as specified in state statutes or the APA Ethical Code. HIPAA does not mandate such consents as PHI may be used or disclosed for the purposes of treatment, payment, or healthcare operations as long as this has been explained in the Notice of Privacy Practices given to the client by the covered entity at their first contact. But HIPAA also does not prevent the use of consents for treatment, testing, etc., if that is required by other local rules. Minors pose special issues, with need for assent and defined designated representative.

**Can patients make amendments to their neuropsychological reports?**

Patients now may make requests to amend (not change) their records, but there is no obligation for the neuropsychologist to agree to the request. HIPAA requires neuropsychologists to have written policies and procedures that describe the process for making such requests and the conditions under which such requests can be denied and that are consistent with state laws. Under HIPAA, the client has the right to disagree with this denial and the covered entity then can provide a rebuttal of the notice of disagreement. All of this documentation must be appended to the record, even if the original request to amend was denied. Neuropsychologists may want to consider allowing patients to amend incorrect information in their records if the neuropsychologist is the originator of the records. However, HIPAA does not allow patients to

request changes to other information that is not PHI, such as interpretation or documented history. Patients may request restrictions as to how information is used or disclosed.

**How are psychotherapy notes treated differently under HIPAA?**

HIPAA specifically excepts "Psychotherapy notes," which are narrowly defined in the Privacy Rule as personal interpretive notes of discussions during therapy sessions that are kept separate from the medical record, from the rules governing patients' access to their records. Information about session start/stop times, and summary of diagnosis, treatment plans, progress with treatment, results of clinical tests, symptoms, functional status, and prognosis are not considered psychotherapy notes. Any notes placed in the patient's record regardless of content are no longer considered psychotherapy notes and are available to be accessed by the patient. Again, state laws regarding how psychotherapy notes are treated must be followed.

**What Must Providers include in a Notice Form?**

Under the Privacy Rule, only doctors or other health care providers with a direct treatment relationship with a patient are required to use reasonable efforts to obtain a written acknowledgment from the patient of receipt of the provider's notice of privacy practices. In that notice, direct providers are required to describe in specific detail their uses and disclosures of health information that they will make. So, while the final rule did not require consent, in effect, given the detailed requirements of the notice of privacy practices, direct providers must use their reasonable efforts to obtain acknowledgment that the patient understands the instances under which PHI may be disclosed for treatment, payment and health care operations.

***Research Information***

**How is research defined under HIPAA?**

The Privacy Rule defines research as "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge."

**What are the HIPAA regulations that impact neuropsychological research?**

In the course of conducting research, researchers may obtain, create, use, and/or disclose individually identifiable health information. Under the Privacy Rule, covered entities are permitted to use and disclose PHI for research with individual authorization, or without individual authorization under limited circumstances set forth in the Privacy Rule.

**Are there specific procedures for using PHI in research?**

Yes. Under HIPAA, use and disclosure may occur without patient authorization if the information has been de-identified by someone not involved in the research, there is an approved waiver from an institutional review board (IRB), the information is being used only as a preparatory form of research, or the PHI being used is that of deceased individuals. In other cases, PHI may be used in research when a research participant authorizes use of his or her PHI, providing the authorization satisfies certain specified requirements.

**What specific steps may a neuropsychologist take to use PHI in research without authorization?**

According to HIPAA, to use or disclose PHI without authorization by the research participant, a covered entity must obtain one of the following: 1) documentation that an alteration or waiver of research participants' authorization for use or disclosure of PHI for research purposes has been approved by an Institutional Review Board (IRB) or Privacy Board, 2) representations from the researcher (written or oral) that the PHI is being used or disclosed solely for the purpose of

designing or assessing the feasibility of a study, 3) representations from the researcher that the use or disclosure is being solely sought for research on PHI of decedents (the PHI must be necessary for the research and at the request of the covered entity documentation of the death of the individuals must be provided), 4) a data use agreement between the covered entity and the researcher, pursuant to which the covered entity may disclose a limited data set to the researcher for research, public health, or health care operations.

**If I receive federal funds for my research and comply with the regulations of the FDA and Common Rule , are there additional requirements to comply with HIPAA?**

Yes. Most research involving human subjects operates under the Common Rule (45 CFR Part 46, Subpart A) and/ or the Food and Drug Administration's (FDA) human subject protection regulations (21 CFR parts 50 and 56), which have some provisions that are similar to, but separate from, the Privacy Rule provisions for research. These human subject protection regulations, which apply to most Federally funded and to some privately funded research, include protections to help ensure the privacy of subjects and the confidentiality of information. The Privacy Rule builds upon these existing Federal protections and creates equal standards of privacy protection for both research governed by the existing Federal human subject regulations and for research that is not.

**How do you obtain documentation of a waiver of authorization by an IRB or Privacy Board?**

In the case of a waiver or authorization pursuant to the Privacy Rule, a covered entity may use or disclose PHI if the covered entity has documented all of the following: 1) identification of the IRB or Privacy Board and the date on which the waiver or authorization was approved, 2) a statement that the IRB or Privacy Board has determined that the alteration or waiver of authorization satisfies three criteria specified in the rule, 3) a brief description of the PHI for which use or access has been determined to be necessary by the IRB or Privacy Board, 4) a statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures, and 5) the signature of the chair or other member, as designated by the chair, of the IRB or the Privacy Board.

**What criteria must be satisfied for an IRB or Privacy Board to approve a waiver of authorization under the Privacy Rule?**

A waiver of authorization may be used to conduct records research when researchers are unable to use de-identified information, and the research could not practicably be undertaken if research participants' authorization were required. For an IRB or Privacy Board to approve such a waiver of authorization under the Privacy Rule, the following criteria must be satisfied: 1) the use or disclosure of PHI involves minimal risk to the privacy of individuals based on the presence of three criteria: a) an adequate plan to protect the identifiers from improper use and disclosure, b) an adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law, and c) adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the project, or for other research for which the use or disclosure of PHI would be permitted; 2) the research could not practicably be conducted without the waiver or alteration; and 3) the research could not practicably be conducted without access to and use of the PHI.

**What provisions must a data use agreement contain?**

Under the Privacy Rule, a data use agreement may be used to allow the covered entity to disclose a limited data set to a researcher or public health or health care operator. The data use agreement must: 1) establish the permitted uses and disclosures of the limited data set by the recipient

consistent with the purposes of the research (which may not include any use or disclosure that would violate the Privacy Rule if done by the covered entity), 2) limit who can use or receive the data, and 3) require the recipient to agree to the following: a) not to use or disclose the information other than as permitted by the agreement or as required by law, b) use appropriate safeguards to prevent the use or disclosure of the information, c) report any uses or disclosures not provided for in the agreement of which the recipient becomes aware, d) ensure that any agents, including a subcontractor, to whom the recipient provides the limited data set agrees to the same restrictions and conditions that apply to the recipient with respect to the limited data set, and d) not identify the information or contact the individual.

**How do I obtain individual authorization for research use of PHI?**

The Privacy Rule permits covered entities to disclose PHI for research purposes when a research participant authorized the use or disclosure of information about her or himself. For most clinical trials and some records research, the principal investigator of the study will seek authorization. The Privacy Rule has a general set of authorization requirements that apply to all uses and disclosures, including for research. However, several special provisions apply to research authorizations.

**How do research authorizations differ from other authorizations required by HIPAA?**

An authorization for research purposes, unlike other authorizations, may state that is does not expire, that there is no expiration date or event, or that the authorization continues until "the end of the research study," and the authorization may be combined with a consent to participate in the research, or with any other legal permission related to the research study.

**What do I do if I started my research study prior to the HIPAA compliance dates?**

A covered entity may use and disclose PHI that was created or received for research, either before or after the compliance date, if the covered entity obtained any of the following prior to the compliance date: 1) individual authorization to use PHI for research, 2) informed consent, or 3) a waiver of informed consent by an IRB in accordance with the Common Rule or an exception under FDA's human subject protection regulations. However, if a waiver of informed consent was obtained prior to the compliance date, but informed consent is subsequently sought after the compliance date, an individual authorization must then be obtained.

## GLOSSARY

*Authorization*= use of PHI for purposes other than treatment, payment, or health care operations also requires written patient authorization to release the information.

*Consent* = patient's consent may be obtained prior to using PHI to carry out treatment, payment, and health care operations; must include patient's right to revoke consent in writing; separate from informed consent for treatment or testing.

*Covered entities*= health plans, healthcare clearinghouses, business associates, and health care providers who electronically transmit any health information in connection with transactions for which the Department of Health and Human Services (HHS) has adopted standards. Researchers are covered entities if they are also health care providers who electronically transmit PHI in connection with any transaction for which HHS had adopted a standard.

*Contrary state laws*= state laws that conflict with HIPAA; laws offering less privacy protection are superceded by the Privacy Rule of HIPAA. (Note: There are 4 exceptions.)

*De-identified information*= data that contain no identifiers of an individual, of relatives, employers, or household members. This information is removed from a data set.

*Disclosure*= release, transfer, provision or access to, or divulging in any other manner of information outside the entity holding the information.

*Electronic transmission*= internet, extranet, leased lines, dial-up lines, private networks, and those transmissions that are physically moved from one location to another (via magnetic tape, disk, or compact disk medium), faxes generated on a computer or sent via a computer, any fax received since electronic source is unknown.

*Limited data set*= data that exclude specified direct identifiers of the individual or relatives, employers, or household members of the individual

*Health information and Protected health information*= HIPAA defines health information as any information (oral or recorded in any form or medium) that is: 1) created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and 2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

While HIPPA's primary privacy concern is health information transmitted by or maintained in electronic media, the Privacy Rule also reaches to data transmitted or maintained in any other form or medium by covered entities. That includes paper records, fax documents and all oral communications. (HIPAA security, identifier, and transaction and code set rules, by contrast, only cover electronic information.)

Protected health information (PHI) under HIPAA means individually identifiable health information. Identifiable refers not only to data that is explicitly linked to a particular individual (that's identified information). It also includes health information with data that reasonably could be expected to allow individual identification.

*Psychotherapy Notes*= Personal interpretive notes of discussions during therapy sessions.

*Use*= sharing, employment, application, utilization, examination, or analysis of individually identifiable health information within an entity that maintains such information.

*For more information:*
http://www.cms/hhs.gov/hipaa/hipaa2/regulations/transactions/finalrule/txfinal.pdf
http://www.hhs.gov/ocr/combinedregtext.pdf
http://www.APApractice.org
http://cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp