**American Academy of Pediatrics**

**HIPAA Privacy Rules**

1. **All data submitted for the Project must be de-identified and must NOT contain protected health information (PHI). Instructions are provided below.**

Under the Health Insurance Portability and Accountability Act of 1996 and the accompanying Privacy Rule regulations, the American Academy of Pediatrics is not considered a covered entity because it is not a health care provider, health plan, or a health care clearinghouse. However, to help protect AAP members who are involved in AAP projects, the AAP Institutional Review Board reviews projects for consistency with HIPAA regulations and serves as a privacy board for consideration of requests for waivers and alterations to the HIPAA authorization requirements.

The AAP wants to make sure that the activities in AAP projects do not place a participant in violation of HIPAA regulations. The Privacy Rule does not apply to de-identified information, however, it is important for the IRB to make sure that your submissions meet specific criteria for de-identification. The Privacy Rule definition extends beyond the definitions generally employed through the Common Rule. Protected health information is defined as individually identifiable health information that a covered entity creates or receives. This includes information about the past, present, or future physical or mental health of a person, provision of health care to a person, and payment for care regardless of whether the information is in written, electronic, or oral form.

Failure to comply with HIPAA can result in civil and criminal penalties (42 USC § 1320d-5). The “American Recovery and Reinvestment Act of 2009” (ARRA) that was signed into law on February 17, 2009, established a tiered civil penalty structure for HIPAA violations. Civil violations can result in penalties of $100 to $50,000 per violation or more, with an annual maximum of $1.5 million. Criminal Penalties apply to covered entities and specified individuals, who "knowingly" obtain or disclose individually identifiable health information in violation of the Administrative Simplification Regulations with imprisonment up to one year. Offenses committed under false pretenses allow penalties to be increased to a $100,000 fine, with up to five years in prison. Offenses committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain or malicious harm permit fines of $250,000, and imprisonment for up to ten years. The Department of Health and Human Services (DHHS) has the authority to exclude from participation in Medicare any covered entity that was not compliant with the transaction and code set standards by October 16, 2003 (where an extension was obtained and the covered entity is not small) (68 FR 48805).

1. **You must remove allof the following 18 elements of HIPAA protected health information listed below from your files with text and photographic images** **before submission. All identifying information must be removed or obscured from written consultation and images prior to submission as described below. The Project Coordinator will review all submissions and will destroy all materials that have not been properly de-identified. Failure to comply with these rules will result in loss of any files which are improperly submitted, may preclude your participation in the project, and may result in loss of your registration fee and/or civil and criminal sanctions under federal regulations (42 USC § 1320d-5).**

Personal Health Information (PHI) is defined as the following identifiers of the individual or of relatives, employers, or household members of the individual (<https://hipaa.com/?p=1718>):

1. Names
2. Geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including dates of admission, discharge, birth, and death.  For persons > 89 years, year of birth cannot be used.
4. Telephone numbers.
5. Fax numbers.
6. Electronic mail address.
7. Social security number.
8. Medical record numbers.
9. Health plan beneficiary numbers.
10. Account numbers.
11. Certificate/license numbers.
12. Vehicle identification and serial numbers including license plates.
13. Device identifiers and serial numbers.
14. Web URLs.
15. Internet protocol addresses.
16. Biometric identifiers, including fingerprints and voice recordings.
17. Full face photos and comparable images.
18. Any other unique identifying number, characteristic, or code.
19. **In addition, while all materials submitted are to be de-identified and Protected Health Information removed, reviewers should be aware that several steps have been taken in the project platform to protect the privacy of any information submitted.** Theframework, applications and data center comply with the Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules to ensure all patient information remains protected and confidential ensuring data or information is not made available or disclosed to unauthorized persons or processes. All electronic features and functionality adhere to strict privacy and security rules regarding Protected Health Information (PHI) at three levels:
20. Access (administrative) controls;
21. Physical elements that provide safeguards, measures, policies and procedures to protect electronic information systems and equipment, from natural and environmental hazards and unauthorized intrusion;
22. Technical safeguards such as policy and procedures for authentication, encryption in transit and at rest that protect electronic health information and control access to it.

**IV. Options given to clinicians for the de-identification of files for this project:**

1. For a DOC (Word) or DOCX file:

Manually remove text and re-save as a DOC, DOCX or PDF;

Cover the text with the highlight color of black, and re-save as a PDF;

Print out the report, completely black out the text with a black magic marker, and rescan the document to a PDF.

2. For a PDF (Adobe) file:

Manually remove text using Adobe and resave as a PDF;

Cover the text with the highlight color of black, and re-save as a PDF;

Print out the report, completely black out the text with a black magic marker, and rescan the document to a PDF.

3. For a paper document:

Print out the report, completely black out the text with a black magic marker, and rescan the document to a PDF.

4. For a photo:

Manually cut out all portions of photos that include labels with identifying information, full face images, or comparable images.

Refer to [How to Deidentify Images in Paint](http://bit.ly/3545OiI) (in your Clinician Guide and at <http://bit.ly/3545OiI>) for specific editing steps.

**V. Clinicians participants have been asked to verify that they agree with the following statements regarding the removal of protected health information before submission:**

1. I have received training and understand my responsibilities under the Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules;
2. I will remove all of the 18 elements of HIPAA protected health information from both my text and image files before submission;
3. I understand that all materials I submit will be reviewed, and any materials found to have Protected Health Information will be destroyed and removed from the XFIN project platform, and I will be asked to resubmit properly de-identified files to continue in the project;
4. I understand that failure to comply with these rules will result in loss of any files which are improperly submitted, may preclude my participation in the project, and may result in loss of my registration fee and/or civil and criminal sanctions under federal regulations (42 USC § 1320d-5).