

New York State Psychiatric Association, Inc.
Area II Council of the American Psychiatric Association
400 Garden City Plaza, Garden City, N.Y. 11530 • (516) 542-0077

Updated January 26, 2010

DIRECTIONS FOR ADOPTING REVISED HIPAA DOCUMENTS

The Health Information Technology for Economic and Clinical Health Act ("HITECH"), enacted in February 2009 as part of the federal economic stimulus package, made extensive changes and clarifications to the HIPAA privacy and security regulations. The majority of the revisions go into effect on **February 17, 2010**, which is one year from the HITECH enactment date. To assist members, NYSPA has prepared revised model HIPAA documents that should be adopted by all HIPAA providers in accordance with the below instructions. For a more extensive summary of the HITECH changes, please refer to *NYSPA Guidance Document: Summary of Health Information Technology for Economic and Clinical Health Act*, also available on the NYSPA web site.

These Directions provide information about the following four documents:

1. Revised Model Policies and Procedures
2. Revised Model Notice of Privacy Practices
3. Revised Model Business Associate Agreement
4. New Model Notice of Breach of Health Information

I. REVISED MODEL POLICIES AND PROCEDURES

All HIPAA providers must adopt policies and procedures implementing the standards and requirements of the HIPAA Privacy and Security Rules. You must maintain these policies and procedures in written or electronic form, and maintain any communications or documentation required under the policies and procedures for no less than six years.

Instructions for tailoring the Revised Model Policies and Procedures for your individual practice

1. At the top of the first page, enter your name or the name of your practice group. You may wish to use the corporate name of your practice, if applicable (e.g., "John R. Doe, M.D., P.C.").
2. Section II, Designation of Privacy Officer. Enter the name of the individual who has been designated as your Privacy Officer. All covered entities under HIPAA must designate a Privacy Officer who will serve as the contact person for all HIPAA-related inquiries. If you have no staff or employees, you will be the Privacy Officer. However, if you have employees, an employee may be designated as the Privacy Officer.

II. REVISED MODEL NOTICE OF PRIVACY PRACTICES

HIPAA providers do **not** need to provide a copy of their new Notice of Privacy Practices to **existing** patients on or before the February 17, 2010 deadline. Similarly, providers do not need to obtain written acknowledgment from each existing patient. Instead, providers must follow these steps:

1. Have the notice available at the service delivery site for individuals to request to take with them; and
2. Post the notice in a clear and conspicuous location at the service delivery site and on the practice website, where applicable.

Providers must, however, distribute the revised Notice of Privacy Practices to all **new** patients seen on or after February 17, 2010 and endeavor to obtain acknowledgment from each new patient.

Instructions for tailoring the Revised Model Notice to your individual practice

1. At the top of the first page, on the blank line, enter your name or the name of your practice group. You may wish to use the corporate name of your practice, if applicable (e.g., "John R. Doe, M.D., P.C.").
2. Section II, Contact Information. Please provide the address, telephone number, fax number and email address, if available, for your medical office.
3. Section IX, Effective Date. We have entered February 17, 2010 as the effective date of the Notice. However, if you change the Notice at any time in the future, you must provide a new effective date.

III. REVISED MODEL BUSINESS ASSOCIATE AGREEMENT

The term "business associate" refers to all vendors, outside companies or consultants you do business with who may receive protected health information in the performance of their duties for you. You must enter into a business associate agreement with each vendor or contractor you hire. In addition, recent changes to HIPAA clarify that any organization that provides data transmissions services, such as a health information exchange organization, a regional health information organization, an e-prescribing gateway or any vendor that offers a personal electronic health record to patients is also to be treated as a business associate.

Because the new HIPAA rules include material changes to the rights and obligations of business associates, all business associate agreements must be revised. You must enter into the new model business associate agreement with all of your current business associates no later than February 17, 2010 and with all new vendors/contractors at the time of engagement. It is

permissible to use the revised agreement for any vendors/contractors that perform work for you between the date of this document and February 17, 2010. Providers should use the revised model business associate agreement for any vendors engaged after February 17, 2010.

The revised model business associate agreement also includes provisions addressing business associates' obligations with respect to the federal False Claims Act and the federal Red Flags Rule.

Instructions for tailoring the Revised Model Business Associate Agreement

1. In the first paragraph, enter the name of each party and the effective date of the agreement. The effective date should be no later than February 17, 2010. Enter your name or the name of your practice in the blank for Covered Entity and the name of your vendor or contractor in the blank for Business Associate.
2. Section 2, Permitted Uses and Disclosures. Check off the type of services that the business associate will provide for your practice. If "other," please write or type in the services to be provided.
4. At the very end of the document, each party must sign where indicated. Many psychiatrists are solo practitioners who do not have corporate names or other business partners. If you fall into this category, enter your name on the first line and sign on the second line. You do not need to fill in the third line. However, if you participate in a partnership or have incorporated your practice, enter the corporate or partnership name of your practice on the first line. Sign your name on the second line. On the third line, print your name and your corporate or partnership title.

IV. NEW MODEL NOTICE OF BREACH OF HEALTH INFORMATION

HITECH requires HIPAA providers to provide written notice to individuals in the event that unsecured personal health information maintained about that individual is breached and the provider determines that the breach poses a risk of significant harm to the individual. Providers must adopt a form of Notice of Breach, which is to be used only in the event of a breach. This new rule applies to all breaches occurring on or after September 23, 2009.

NYSPA has prepared a model Notice of Breach for use by members in the unlikely event that patient information is breached by an unauthorized third party. This model Notice of Breach will be sufficient to comply with both the new federal requirement and current New York State law on breach of personal information.

Instructions for Tailoring the Notice of Breach in the Event of an Actual Breach

1. At the top of page 1, enter your name, practice name, address, phone number and email address, if available. Also enter the name, address and salutation for individual receiving the Notice of Breach.

2. Under Paragraph 1, insert name of physician or practice name.
3. Under Paragraph 2, insert name of individual whose information was breached.
4. Under Paragraph 3, provide a brief description of the circumstances surrounding the breach.
5. Under Paragraph 4, insert date breach occurred, if known to you.
6. Under Paragraph 5, insert the date you discovered the breach.
7. Under Paragraph 6, place a check next to each type of information breached.
8. Under Paragraph 9, insert your contact information.

The required Notice of Breach must be sent without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. A breach will be treated as discovered by the covered entity as of the first day on which the breach is known to the covered entity or would have been known to a covered entity exercising reasonable diligence. The notice must be sent by first-class mail or by email, if the individual has specified a preference for communication by email.

****Any NYSPA members who experience a breach of unsecured patient information are advised to contact NYSPA Central Office for guidance before taking further action.**

V. DISCLAIMER

This information and the sample forms are copyrighted material for the use of NYSPA members only in complying with the federal HIPAA privacy and security regulations and may not be copied, distributed or disseminated for any purpose other than the use of our members in their private medical practices. This information is provided solely for general informational purposes and does not constitute, and should not be relied upon as, legal advice. Members should consult with attorneys to evaluate their specific circumstances and obtain customized advice. While all reasonable attempts have been made to ensure the accuracy, completeness, and timeliness of this information, the NYSPA disclaims any express or implied representations or warranties as to the accuracy, completeness or timeliness of this information for any purpose or suitability of this information for any particular use. Members using this information assume full responsibility for their use of it and agree that the NYSPA is not liable for any claim, loss or damage arising from any member's use or reliance upon this information.

