MSMS
MICHIGAN STATE MEDICAL SOCIETY

HIPAA GUIDE

FOR PHYSICIAN PRACTICES

JANUARY 2026 EDITION

msms.org

TABLE OF CONTENTS

MSMS
MICHIGAN STATE MEDICAL SOCIETY

HIPAA OVERVIEW

1

The Health Insurance Portability and Accountability Act (HIPAA) regulates several aspects of the delivery of and payment for health care. One of HIPAA's primary objectives was to protect and federally regulate on a uniform basis the use and disclosure of Protected Health Information (PHI). Virtually all of the information contained in a typical medical record would be considered PHI and therefore regulated by HIPAA.

Pursuant to HIPAA's statutory mandate, the Department of Health and Human Services (HHS) issued the "Privacy Rule," which establishes national standards to protect individual medical records and other PHI, and the "Security Rule," which establishes administrative, physical and technical safeguards to protect the confidentiality, integrity and security of electronic PHI.

In 2009, Congress significantly amended portions of the Privacy Rule and the Security Rule by passing the Health Information Technology for Economic and Clinical Health Act (HITECH Act).

The HITECH Act:

- extended the applicability of certain Privacy Rule and Security Rule provisions to Business Associates;
- added mandatory notification requirements in the event of breaches of unsecured PHI;
- created new limitations on the use and disclosure of PHI for marketing and fundraising;
- prohibited the sale of PHI;
- required the consideration of a limited data set as the minimum necessary amount to be disclosed for a particular use or disclosure of PHI;
- expanded patient right of access to PHI and the right to receive an accounting of disclosures of their PHI and to request restrictions; and
- expanded and strengthened enforcement provisions.

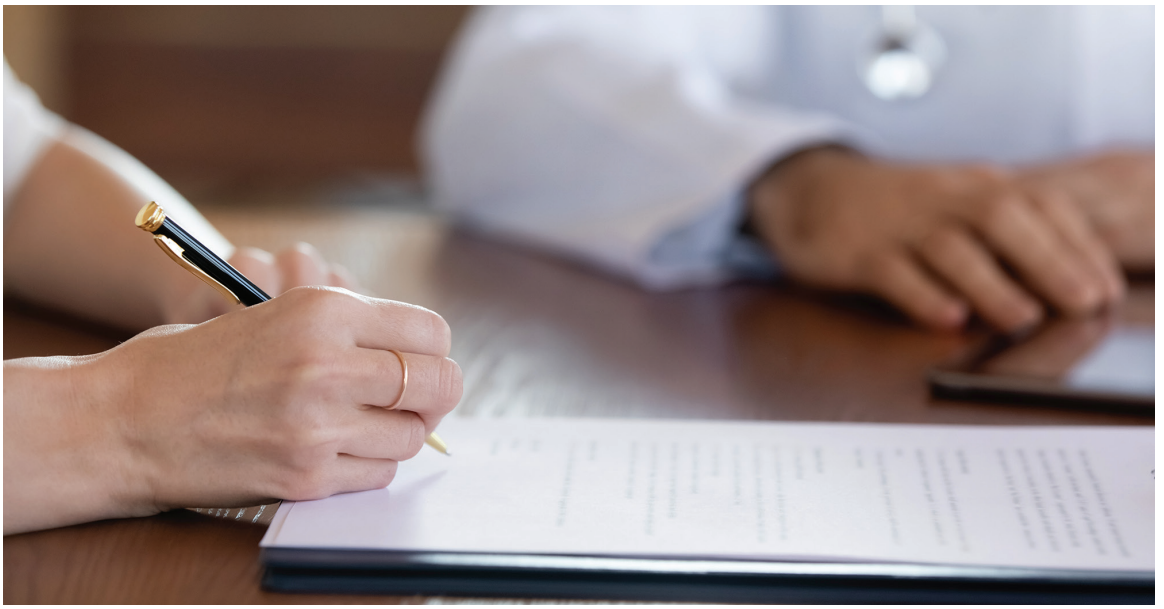
In 2013, the Department of Health and Human Services, Office for Civil Rights (OCR) published its final rule providing for modifications to the HIPAA privacy, security, enforcement, and breach notification rules under the HITECH Act and the Genetic Information Nondiscrimination Act, and other modifications to the HIPAA rules (the "Omnibus Final Rule"). The Omnibus Final Rule became effective March 26, 2013.

On January 21, 2021, HHS published a Notice of Proposed Rule-making which identified several proposed changes to the Privacy Rule to support and remove barriers to coordinated care and individual engagement. As of this publication date, a Final Rule implementing these proposed changes has not yet been issued.

On April 26, 2024, OCR issued a Final Rule which amended certain provisions of the Privacy Rule to strengthen privacy protections for PHI related to lawful reproductive health care and the confidentiality of substance use disorder records covered under 42 CFR Part ("Part2"). This Final Rule became effective June 25, 2024 with certain requirements regarding changes to Notices of Privacy Practices to be implemented effective February 16, 2026.

On June 18, 2025, a federal district court issued a nationwide order in *Purl et al. v. Department of Health & Human Services* vacating the Final Rule provisions addressing reproductive health care information. On September 10, 2025, the U.S. Court of Appeals for the Fifth Circuit dismissed an appeal of the federal court ruling, leaving the vacating order in place. Accordingly, Covered Entities do not need to comply with the Final Rule provisions regarding reproductive health information. However, the court did not disturb the Final Rule's changes to the Notice of Privacy Practices requirements addressing substance use disorder treatment records covered under Part 2. Accordingly, Covered Entities must still update their Notice of Privacy Practices by February 16, 2026 to address limitations on the use and disclosure of PHI from certain substance use disorder treatment programs subject to Part 2.

This guide explains and provides generalized forms for your use in complying with the Privacy Rule and the Security Rule, each as amended by the HITECH Act and the Omnibus Final Rule.



SHUTTERSTOCK: ROSTISLAV_SEDLACEK

THE PRIVACY RULE

2

The HIPAA Privacy Rule establishes a series of standards addressing the use and disclosure of an individual's PHI by physicians and other providers and organizations subject to the Privacy Rule (e.g., Covered Entities and Business Associates). It also establishes standards for individual privacy rights and how health information is used. Generally, a Covered Entity (or Business Associate) cannot use or disclose PHI except as the Privacy Rule permits or requires. This Chapter summarizes the key requirements under the Privacy Rule and actions physicians should take to ensure their practices are in compliance with the Privacy Rule.

Covered Transactions

HIPAA applies to Covered Entities (health plans, health care clearinghouses and healthcare providers) which transmit health information in electronic form in connection with certain covered transactions. A "covered transaction" means the transmission of information between two parties to carry out financial or administrative activities related to healthcare, including:

- Health care claims or equivalent encounter information;
- Healthcare payment and remittance advice;
- Coordination of benefits;
- Health care claim status;
- Enrollment and disenrollment in a health plan;
- Eligibility for a health plan;
- Health plan premium payments;
- Referral certification and authorization;
- First report of injury;
- Health claims attachments;
- Health care electronic funds transfers (EFT) and remittance advice; and
- Other transactions that the Secretary may prescribe by regulation.

Notice of Privacy Practices

The Privacy Rule requires you to prepare and distribute a form entitled "Notice of Privacy Practices." A Notice of Privacy Practices (NPP) informs individuals of the uses and disclosures of PHI that may be made by your practice and of an individual's rights and the practice's legal duties with respect to PHI.

The NPP must be provided at the patient's initial visit to your practice and at any time upon request. A copy of the NPP must be posted in a prominent location in your office and on your website if you have one. You must also retain copies of the NPP issued by your practice, including copies of any revised NPPs.

A sample NPP form (Form 1) is available at msms.org/HIPAASampleForms. Form 1 includes a statement relative to uses and disclosures of psychotherapy notes, but you are not required to include this in your NPP if you do not record psychotherapy notes. Form 1 also excludes the statement required for Covered Entities which intend to engage in fundraising communications, as physician medical practices typically will not engage in such activities.

In addition to distributing/posting the NPP, the Privacy Rule requires that you make a good faith effort to obtain a signature from the patient acknowledging his or her receipt of the NPP. HHS did not specify the exact form of this acknowledgment. Instead, HHS only required that the acknowledgment be in writing, intending that you choose the form and other details of theacknowledgment that are best suited to your practice. If the patient fails or refuses to sign the acknowledgment, you must document the practice's good faith efforts to obtain such written acknowledgment.

Therefore, to ensure compliance with the NPP acknowledgment requirement, each patient's medical record should contain either: (i) an acknowledgment signed by the patient; or (ii) documentation that a good faith effort to obtain a signed acknowledgment was made and that the patient refused to sign the acknowledgment (such documentation can be included within the acknowledgment form). **A sample acknowledgment form (Form 2) is available at msms.org/HIPAASampleForms.**

Once you have distributed/posted your NPP and complied with the acknowledgment requirement, you are permitted to use and disclose the patient's PHI for treatment, payment and health care operations purposes without further authorization from the patient.

SHUTTERSTOCK; THE CORGI

Notice of Privacy Practices: Frequently Asked Questions

Why are there so many different notices of privacy practices in circulation? Some seem longer than others. Isn't there a uniform notice of privacy practices?

Although each NPP must meet the minimum standards required by the Privacy Rule, the content of each NPP may sometimes vary based on the specific functions, uses and disclosures by each Covered Entity. The Privacy Rule's NPP standards provide Covered Entities certain flexibility and discretion—there is no "one size fits all" approach.

What obligations do physicians and other health care providers have to comply with the notice of privacy practices requirement?

A "covered health care provider" that has a direct treatment relationship with an individual must provide the NPP no later than the date of the first service delivery (including service delivered electronically) to the individual. However, in an emergency treatment situation, the NPP must be given as soon as reasonably practicable after the emergency treatment. Covered health care providers must also make a good faith effort to obtain a written acknowledgment of receipt of the NPP, and if not obtained, document its good faith efforts to obtain such acknowledgment and the reason why the acknowledgment was not obtained.

If the covered health care provider maintains a physical service delivery site, it must have the NPP available at the site for individuals to request to take with them. In addition, it must post the NPP in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered health care provider to be able to read the notice. Providers may post a summary of the NPP as long as the full notice is immediately available (such as on a table directly under the posted summary) for individuals to pick up without any additional burden on their part. The government's position is that it would not be appropriate to require an individual to have to ask the receptionist for a copy of the full NPP.

Can the notice of privacy practices be given by e-mail or other electronic means?

Yes, the NPP may be provided to an individual by e-mail or other electronic means, if the individual agrees to electronic notice and such agreement has not been withdrawn. The individual's agreement to electronic notice can be obtained electronically. Even if the individual receives the NPP electronically, the individual retains the right to obtain a paper copy of the NPP from the covered health care provider upon request. If the covered health care provider knows that the electronic transmission has failed, a paper copy of the notice must be provided to the individual. Regardless of the method of transmission, a covered health care provider must still make a good faith effort to obtain a written acknowledgment of the individual's receipt of the NPP or document its good faith efforts to obtain the acknowledgment and the reason why it was not obtained.

If the first service delivery to an individual is delivered electronically (e.g., telemedicine) and if the individual has agreed to receipt by e-mail, the health care provider must provide electronic notice automatically and contemporaneously in response to the individual's first request for service.

Notice of Privacy: Frequently Asked Questions (continued)

What must a physician's practice do if it revises its notice of privacy practices?

When a practice revises its NPP, the revised NPP must be made available upon request on or after the effective date of the revision. The revised NPP must also be made available at the physical delivery site and posted in a clear and prominent location. Physician practices are not required to print and hand out a revised NPP to all individuals seeking treatment; practices are only required to give a copy of the NPP to, and obtain a good faith acknowledgment of receipt from, new patients. There is no requirement to e-mail the revised NPP to patients who have elected to receive the NPP via e-mail. Practices should also post the updated NPP on their websites.

What obligations do physicians and other Covered Entities have to individuals with disabilities relative to the Notice of Privacy Practices requirement?

To the extent a Covered Entity is required to comply with Section 504 of the Rehabilitation Act of 1973 or the Americans with Disabilities Act of 1990, the Covered Entity has an obligation to take steps that may be necessary to ensure effective communication with individuals with disabilities, which could include making the NPP available in alternate formats, such as Braille, large print, or audio.

What about limited English proficiency patients?

In accordance with Title VI of the Civil Rights Act of 1964 and Section 1557 of the Affordable Care Act, nearly all Covered Entities are required to take reasonable steps to ensure meaningful access for limited English proficient persons to the services of the Covered Entity, which could include translating the NPP into frequently encountered languages.

Are practices required to obtain a patient's signature on the Notice of Privacy Practices Acknowledgment Form?

No. You are not required to obtain a patient's signature on the NPP Acknowledgment form. Instead, you are required to ask patients to sign the acknowledgment and if, for whatever reason, the patient refuses, you should document in the patient's record that a good faith effort was made and the patient refused to sign.

Are there any new changes to the Notice of Privacy Practices requirement?

Yes. By February 16, 2026, physicians and other Covered Entities must update their Notice of Privacy Practices to incorporate new requirements regarding the use and disclosure of substance use disorder treatment records received from programs subject to 42 CFR part 2 as reflected in the April 2024 Final Rule.

The Minimum Necessary Standard

When the use or disclosure of PHI is allowed, the Privacy Rule requires that reasonable efforts be used to limit the use and disclosure of PHI to the minimum amount necessary to accomplish the intended purpose of the use or disclosure. The minimum necessary standard requires Covered Entities to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of PHI.

The minimum necessary standard does not apply to uses and disclosures of PHI:

- to the individual who is the subject of the PHI;
- for treatment purposes;
- pursuant to an Authorization; or
- if required by law.

The minimum necessary standard does apply to uses and disclosures of PHI for payment and health care operations purposes.

To comply with the minimum necessary standard, you are required to identify: (i) the persons or classes of persons within your practice who need access to PHI to carry out their duties; (ii) the categories of PHI for which access is needed; and (iii) the appropriate conditions and limitations to such access applicable to each person or class of persons. To ensure compliance, you must conduct this identification process and document in writing in a compliance plan or in your practice's corporate records that you did so along with any alterations made to your office procedures as a result. In addition, the HITECH ACT states that to meet the minimum necessary standard a "limited data set" of PHI should be used when practicable. To be a "limited data set," the PHI used or disclosed should exclude direct patient identifiers (and identifiers of the patient's relatives, employer or members of the patient's household). Such direct identifiers include names, addresses, all elements of dates (e.g., birth date, admission/discharge dates, date of death, etc.), telephone numbers, fax numbers, e-mail addresses, social security numbers, medical record numbers, health plan beneficiary numbers, account numbers, certificate/license numbers, vehicle identifiers and serial numbers (including license plate numbers), device identifiers or serial numbers, URLs, internet addresses, biometric identifiers (including finger and voice prints) and identifying photographic images of patients.

The HITECH Act requires HHS to issue guidance on what constitutes minimum necessary. To date, this guidance has not been published. Until HHS issues further guidance, you should limit uses and disclosures to no more than the "limited data set" described above, when practicable.

HIPAA Authorization Form

If you plan to use or disclose PHI for any purpose (e.g., research, fundraising, etc.) other than for treatment, payment or health care operations, the Privacy Rule requires that you first obtain a signed authorization (not to be confused with the Notice of Privacy Practices Acknowledgment, discussed above) from the patient unless an exception applies. The exceptions are uses or disclosures:

A. Which are required by HIPAA, including:
    i. Subject to certain limitations and conditions, to an individual or his or her personal representative if the individual or his or her personal representative specifically requests access to PHI, or an accounting of disclosures of the individual's PHI; and
    ii. To the Department of Health and Human Services when it is undertaking a compliance investigation or review of enforcement action.

B. Subject to certain limitations and conditions, for uses and disclosures required by law to the extent that such use or disclosure complies with and is limited to the relevant requirements of such law.

C. For public health activities and purposes, including to:
    i. A public health authority that is authorized to collect information for the purpose of preventing or controlling disease, injuries or disabilities.
    ii. A public health authority or other appropriate government authority to report child abuse if the authority is legally authorized to receive such reports.
    iii. A person or entity subject to the jurisdiction of the Food and Drug Administration about the quality, safety or effectiveness of an FDA-regulated product or activity for which the person or entity has responsibility.
    iv. To notify a person whom may have been exposed to a communicable disease or may otherwise be at that risk of contracting or spreading a disease or condition, as permitted by law to carry out a public health intervention or investigation.
    v. An employer under limited circumstances and conditions where the employee needs the information to comply with the Occupational Safety and Health Administration or the Mine Safety and Health Administration requirements.
    vi. A school to the extent the information disclosed is limited to proof of immunizations and the school is required by law to have proof of immunization prior to admitting the individual, and if you document the agreement to the disclosure from either the individual (if an adult or emancipated minor) or the individual's parent, guardian or other person acting in loco parentis of the individual (if the individual is minor).

D. To a government authority, including a social service or protective service agency authorized by law, under limited circumstances and conditions, for the purpose of reporting abuse, neglect or domestic violence.

E. To a health oversight agency for certain health oversight activities authorized by law.

F. In response to an order of court or other lawful process for judicial and administrative proceedings under limited circumstances and conditions.

G. To a law enforcement official for certain law enforcement processes under limited circumstances and conditions.

H. To a coroner, medical examiner for the purpose of identifying a deceased person, determining a cause of death, other duties authorized by law, or to a funeral director as necessary to carry out their duties with respect to the decedent.

I. For cadaveric organ, eye or tissue donation purposes.

J. For research purposes, under limited circumstances and conditions.

K. To the extent the use or disclosure is consistent with applicable law and standards of ethical conduct, to avert a serious threat to health or safety under limited circumstances and conditions;

L. For certain specialized government functions;

M. As authorized and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provides benefits for work-related injuries or illness without regard to fault.

The Privacy Rule allows the use of a single Authorization form regardless of the use or disclosure of the medical information contemplated by the authorization so long as it contains certain required information. **A sample Authorization (Form 3) is available at msms.org/HIPAASampleForms.** Before disclosing PHI, whether pursuant to an Authorization or an exception under the Privacy Rule, you should confirm that such disclosure is also in compliance with other applicable state and federal privacy laws and regulations. For example, disclosures of information that might directly or indirectly identify a patient as having or having had a substance use disorder are subject to heightened privacy and disclosure requirements pursuant to 42 CFR Part 2.

SHUTTERSTOCK: MARIDAV

Identify "Business Associates"

In addition to Covered Entities, Business Associates are fully subject to the Privacy Rule and the Security Rule. This means that the Privacy Rule and Security Rule may be directly enforced against a Business Associate. HIPAA defines "Business Associate" to mean, with respect to a Covered Entity, a person who creates, receives, maintains or transmits PHI on behalf of the Covered Entity for a function or activity regulated by HIPAA, including, but not limited to, claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, certain patient safety activities, billing, benefit management, practice management and repricing. A Business Associate also includes a person who provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services to or for such Covered Entity where the provision of the service involves the disclosure of PHI from the Covered Entity or from another Business Associate of the Covered Entity. A Business Associate does not include members of the Covered Entity's workforce, including the Covered Entity's employees, volunteers, trainees, and other persons whose conduct is under the direct control of the Covered Entity, whether or not they are paid by the Covered Entity.

To the extent that a Business Associate is to carry out a Covered Entity's obligation under HIPAA, the Business Associate must comply with the requirements of the Privacy Rule that apply to the Covered Entity in the performance of the obligation. The Omnibus Final Rule implements provisions of the HITECH Act making Business Associates of Covered Entities, and subcontractors of Business Associates, directly liable for compliance with certain of the requirements of the HIPAA Privacy Rule and Security Rule. The Omnibus Final Rule confirms that a Business Associate is permitted to disclose protected health information to a Business Associate that is a subcontractor, and to allow the subcontractor to create or receive protected health information on its behalf, if the Business Associate obtains the required satisfactory assurances that the subcontractor will appropriately safeguard the information. The Omnibus Final Rule confirms that a Covered Entity is not required to obtain satisfactory assurances from Business Associates which are subcontractors. Rather, a Business Associate is required to obtain such assurances from its subcontractor. Business Associates must ensure that any subcontractors that create or receive protected health information on behalf of the Business Associate agree to the same restrictions and conditions that apply to the Business Associate with respect to such information. A Business Associate aware of noncompliance by its Business Associates subcontractor is required to respond to the situation in the same manner as a Covered Entity that is aware of noncompliance by its Business Associate.

Covered Entities must identify their Business Associates and ensure that they have entered into a written agreement with the Business Associate which meets certain requirements, known as a "Business Associate Agreement" (discussed below). Business Associates are also required to enter into Business Associate Agreements or other arrangements that comply with the Privacy Rule and Security Rule with their Business Associate subcontractors.

Business Associate Agreements

Despite the fact that the HITECH Act made Business Associates subject to the Privacy Rule and Security Rule directly, you still must have written agreements with your Business Associates. The following is a list of required and suggested provisions for Business Associate Agreements (taking into account the Privacy Rule, the HITECH Act requirements and the Omnibus Final Rule). HHS has also issued a **Model Business Associate Agreement (Form 4) which is available at msms.org/HIPAASampleForms.**

The HIPAA Privacy Rule, HITECH Act, and the Omnibus Final Rule collectively require that Business Associate Agreements contain or address the following provisions in some form:

A. A definition of the permitted and required uses and disclosures of health information that the Business Associate may make.

B. A requirement that the Business Associate do all of the following:
   - i. Not use or disclose the health information, except as permitted or required by the agreement or as required by law;
   - ii. Use appropriate safeguards and comply, where applicable, with the security standards for the protection of electronic protected health information, to prevent misuse and inappropriate disclosure of the health information;
   - iii. Report to you any unauthorized access to, uses and disclosures of the health information, including any breach of unsecured health information, of which the Business Associate becomes aware without unreasonable delay and in no case later than 30 calendar days after discovery;
   - iv. Require the same disclosure conditions and restrictions that the agreement imposes on the Business Associate on any agents and/or subcontractors of the Business Associates;
   - v. Make the health information available to your patients for access and copying;
   - vi. Make the health information available so that amendments to it can be made as needed and update the health information to include any such amendments;
   - vii. Make available the health information needed to provide an accounting of disclosures of the health information made by the Business Associate (if the Business Associate maintains an electronic health record, an accounting of disclosures from the electronic health record for treatment, payment or health care operations purposes must be maintained for the three (3) year period prior to the request);
   - viii. To the extent the Business Associate is to carry out an obligation of yours under the HIPAA privacy rule, comply with the requirements of the privacy rule that apply to you in the performance of the obligation;
   - ix. Make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the Business Associate on behalf of you, available to HHS for purposes of determining compliance with the privacy rule;
   - x. Return or destroy the health information upon termination of the agreement or, if that is not feasible, extend the protections of the agreement to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible;
   - xi. Authorize termination of the agreement by you, if you determine that the business associate has violated a material term of the agreement;

xii. Not use or disclose health information for fundraising or marketing purposes or sell health information;

xiii. Except as otherwise required by law, not disclose health information to a health plan for payment or health care operations purposes if the patient has requested this special restriction and the health information pertains to an item or service you furnished and you have been paid out of pocket in full for the item or service to which the health information solely relates;

xv. If the Business Associate knows of a pattern of activity or practice by a subcontractor or agent that constitutes a material breach or violation of the subcontractor's obligations under the contract or other arrangement, the Business Associate must take reasonable steps to cure the breach or end the violation, as applicable, and if such steps are unsuccessful, the Business Associate must terminate the contract. Further, the Business Associate shall provide written notice to you of any pattern of activity or practice by the Business Associate, a subcontractor or agent which constitutes a material breach or violation of its obligations under the contract or other arrangement within five (5) days of discovery and shall meet with you to discuss and attempt to resolve the problem as one of the reasonable steps to cure the breach or end the violation;

xvi. Comply with HIPAA's "minimum necessary" requirement by limiting the use or disclosure of health information (i) to the extent practicable, to a limited data set or, (ii) if needed by such entity, to the minimum necessary to accomplish the intended purpose of such use, disclosure, or request, respectively;

xvii. Develop, implement, maintain, and use appropriate safeguards to prevent any use or disclosure of health information other than as provided by this Agreement, and to implement administrative, physical, and technical safeguards as required by Sections 164.308, 164.310, 164.312 and 164.316 of title 45, Code of Federal Regulations and the HITECH Act in order to protect the confidentiality, integrity, and availability of health information that Business Associate, a subcontractor or agent creates, receives, maintains, or transmits, to the same extent as if Business Associate, subcontractor or agent were a Covered Entity; and

xviii. Comply with the additional requirements of Title XIII of the HITECH Act that relate to privacy and security and that are made applicable with respect to Covered Entities, shall also be applicable to the Business Associate, its subcontractors and agents.

C. A provision allowing you to terminate the agreement if the Business Associate, its subcontractor or agent materially breaches the agreement.

In addition to the above provisions, it would be prudent to include in a Business Associate Agreement the following provisions:

A. ***A Right to Cure Business Associate Violations.*** The Privacy Rule states that Covered Entities are not in compliance if they know of a pattern of activity or practice of the Business Associate that constitutes a violation of the Privacy Rules unless the physician takes reasonable steps to cure the breach or end the violation. You should expressly reserve the right in the agreement to cure a violation by the Business Associate. In addition, you should have the right to terminate the agreement and seek related remedies, even if you are able to cure the violation.

B. ***Ownership of Disclosed Health Information.*** The agreement should contain an express, unequivocal statement that, as between the Covered Entity and the Business Associate, the Covered Entity is the owner of all the disclosed health information.

C. ***Responses to Subpoenas.*** The Business Associate should give you notice of the receipt of any subpoena, other discovery request or a judicial or administrative order requiring that the Business Associate disclose information that the Business Associate has received, creates or maintains on behalf of you.

D. ***Indemnification.*** The HITECH Act increased the civil and criminal penalties for Privacy Rule and Security Rule violations and expanded who may seek enforcement for violations (see Chapter 5). Under certain circumstances, you may be liable for a Business Associate's violation. For this reason, it is recommended that you include indemnity and hold harmless provisions in your Business Associate Agreements. The following is sample indemnification language which may be inserted in a Business Associate Agreement:

The Business Associate (the "Indemnitor") shall indemnify, defend and hold [insert name of physician practice] and its directors, officers, shareholders, employees and agents (collectively the "Indemnitee"), harmless from and against any and all claims, costs, liabilities, losses, damages and/or expenses (including, without limitation attorney fees) (collectively "Damages") incurred by the Indemnitee arising out of or relating in any way to: (i) any breach, inaccuracy, failure or violation of any of the representations, warranties, covenants or undertakings of or by the Indemnitor contained in this Agreement; (ii) any violation of any of the requirements contained in the Health Insurance Portability and Accountability Act of 1996 (the "Act") and/or any rules or regulations promulgated pursuant to the Act; and (iii) any violation of any of the requirements contained in the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 ("the HITECH Act") and/or any rules or regulations promulgated pursuant to the HITECH Act.

Importantly, if your contract with a Business Associate contains any provision limiting the liability of the Business Associate in any way, such as a cap on liability equal to the fees paid to the Business Associate pursuant to the contract, an exception should be added excluding any damages related to the Business Associate's violation of HIPAA.

HIPAA Compliance Program

Physicians should ensure that they have and implement a written compliance program in place which, at a minimum, includes certain elements required by the Privacy Rule. **A list of the required elements is included on Form 5 available at msms.org/HIPAASampleForms.**

Patient Requested Restrictions on Disclosures

The HITECH Act and the Omnibus Final Rule requires you to comply with a patient's requests to restrict the disclosure of PHI if the disclosure would be to a health plan and pertains solely to an item or service for which the patient pays you in full out of pocket. For example, if a patient requests you not to disclose to his/her health plan a surgical procedure for which the patient paid you in full out of pocket, you are not permitted to disclose that information.

You are never required to honor a patient request for a restriction if the disclosure is necessary to carry out their treatment.

Accounting for Disclosures

The Privacy Rule requires that you provide patients, upon their request, with an accounting of disclosures you have made of their PHI during the six years prior to the date on which the accounting is requested, except for disclosures:

- For purposes of treatment, payment and health care operations;
- To individuals of PHI about them;
- Incident to a use or disclosure otherwise permitted or required by HIPAA;
- Pursuant to a HIPAA authorization;
- For the facility's directory or to persons involved in the individual's care or other notification purposes under 45 CFR §164.510;
- For national security or intelligence purposes;
- To correctional institutions or law enforcement officials;
- As part of a limited data set in accordance with 45 CFR §164.514€; or
- That occurred prior to the compliance date for the Covered Entity.

The accounting must be provided no later than 60 days after receipt of the request. The accounting must include for each disclosure the date of the disclosure; the name of the entity or person who received the PHI and, if known, the address of such entity or person; a brief description of the PHI disclosed; and a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or, in lieu of such statement, a copy of a written request for a disclosure, if any. The first accounting in any 12 month period must be provided without charge. A reasonable cost-based fee may be imposed for subsequent requests by the same individual within the 12 month period.

If you maintain an electronic health record, the HITECH Act and the Omnibus Final Rule require you, upon a patient request, to provide an accounting of all disclosures (including disclosures made for treatment, payment and health care operations or which are included in one of the above exceptions) during the preceding three years. In addition, the HITECH Act requires you to either: (a) furnish an accounting of disclosures made by your Business Associates; or (b) furnish the requesting patient a list of your Business Associates.

If I maintain an electronic health record, do I have to comply with both accounting requirements under HIPAA and HITECH Act?

Yes. If you maintain an electronic health record and a patient requests an accounting of disclosures, you must provide an accounting of all disclosures during the preceding three years, and an accounting of disclosures which are not subject to an exception under the HIPAA accounting requirement during the preceding six years.

Access to PHI Upon the Patient's Request

The Privacy Rule and Michigan's Medical Records Access Act have always required physicians to grant a right of access to patients so that they may inspect and copy their medical record. In addition, the 21st Century Cures Act and administrative rules promulgated thereunder (e.g., the "Information Blocking Rules") prohibit physicians and other health care providers from engaging in conduct which the provider knows is "unreasonable and likely to interfere with, prevent, or materially discourage access, exchange or use of electronic health information" unless an exception applies. Thus, consideration must be given to both Michigan and federal laws and rules when responding to a request for access to PHI.

The Privacy Rule states that, subject to limited exceptions and circumstances, an individual has a right of access to inspect and obtain a copy of PHI about the individual in a designated record set for as long as the PHI is maintained except for (1) psychotherapy notes, and (2) information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding. Additional exceptions to the Privacy Rule's right of access include circumstances which may or may not be subject to review. For example, PHI may be denied under the following circumstances without providing the individual an opportunity for review:

- A Covered Entity is a correctional institution or a Covered health care provider acting under the direction of the correctional institution may deny, in whole or in part, an inmate's request to obtain a copy of PHI if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.
- If the PHI is created or obtained by a Covered health care provider in the course of research, the individual's right of access to such PHI may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the Covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research.
- If the PHI is subject to the Privacy Act under 5 USC §552a, access may be denied if the denial would meet the requirements of that law.
- If the PHI was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

A Covered Entity may deny an individual access under the following additional circumstances provided that the individual is given a right to have such denials reviewed:

- A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;
- The protected health information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined,

in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or

- The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

If the right of access to PHI is denied under one of the above circumstances, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the Covered Entity to act as a reviewing official and who did not participate in the original decision to deny. The Covered Entity must still provide access to any other PHI requested after excluding the PHI to which the Covered Entity has a ground to deny access. The Covered Entity must also provide a timely written denial to the individual that is written in plain language and contains (1) the basis for the denial; (2) if applicable, a statement of the individual's right to review under the HIPAA Privacy Rule, including a description of how the individual may exercise such review rights, and (3) a description of how the individual may complain to the Covered Entity pursuant to the complaint procedures under 45 CFR §164.530(d) or to the HHS Secretary pursuant to 45 CFR §164.530(a)(1)(ii).

If the individual exercises the right to have the denial reviewed, the Covered Entity must promptly refer the request to the designated reviewing official who must determined, within a reasonable period of time, whether or not to deny the requested access under the Privacy Rule. The Covered Entity must then promptly provide written notice to the individual of the determination of the designated reviewing official and take other action to carry out the designated reviewing official's determination.

Timely Response to Request for Access

The Privacy Rule requires a Covered Entity to act on a request for access to PHI (either acceptance or denial in whole or in part) no later than 30 days after the receipt of the request. If the Covered Entity is unable to take action within 30 days, the Covered Entity may extend the time to respond by no more than 30 days provided that within the initial 30 day period, the Covered Entity provides the individual with a written statement of the reasons for the delay and the day by which the Covered Entity will complete its action on the request, which cannot exceed the 30 day extension.

Importantly, notwithstanding the time afforded under the HIPAA (which is consistent with the time afforded under the Michigan Medical Records Access Act), physicians who maintain an electronic health record should keep in mind that under the Cures Act Information Blocking Rules, a physician may be deemed to be engaging in information blocking if they fail to reasonably respond to the request for access for electronic PHI, even if access is given within the time allowed under HIPAA (e.g., intentionally waiting until the end of the initial 30-day period to respond to a request for access). Accordingly, physicians should ensure that it has policies and protocols in place to timely respond to requests for access to PHI.

Form of Access Requested

A Covered Entity is required to provide the individual with access to the PHI in the form and format requested by the individual, if the PHI is readily producible in such form and format; or if not, in a readable hard copy form or such other form and format as agreed to by the Covered Entity and the individual. For requests for electronically maintained PHI, the HITECH Act and the Omnibus Final Rule modified the Privacy Rule so that if you maintain an electronic health record, the patient has a right to receive the copy in an electronic format and, if the patient chooses, to have the electronic copy transferred directly to a person or entity designated by the patient. Instructions regarding who to transmit the PHI electronically to must be provided to you by the patient in clear, conspicuous, and specific manner.

A Covered Entity may provide an individual with a summary of the PHI requested, in lieu of providing access to the PHI, or may provide an explanation of the PHI to which access has been provided, if (1) the individual agrees in advance to such summary or explanation, and (2) the individual agrees in advance to the fees imposed, if any, by the Covered Entity for such summary or explanation.

Charges for Copies of PHI

The Privacy Rule permits physicians to charge a reasonable, cost-based fee for production of a copy of requested PHI, provided that the fee only includes the cost of:

- Labor for copying the PHI requested by the individual, whether in paper or electronic form;
- Supplies for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media;
- Postage, when the individual has requested the copy, or the summary or explanation, be mailed; and
- Preparing an explanation or summary of the PHI, if requested and agreed to by the individual.

In addition, Michigan's Medical Records Access Act prescribes the maximum fees that may be applied. If charging a fee for paper copies of medical records, it is recommended that physicians utilize this fee schedule, or charge their reasonable costs for production of copies of medical records, whichever is less. For electronic PHI, in lieu of calculating a reasonable cost-based fee, physicians are permitted to charge a flat rate fee of $6.50 per request, inclusive of all labor, supplies, and any applicable postage. HHS has clarified that the $6.50 flat rate fee is not the maximum fee that can be charged for all individual requests for a copy of PHI under the Privacy Rule. Rather, the $6.50 flat rate fee is an option to those entities that do not want to go through the process of calculating the actual or average cost for requests of electronic copies of PHI maintained electronically. The government has further clarified the following:

- Labor costs included in a reasonable cost-based fee could include skilled technical staff time spent to create and copy the electronic file, such as compiling, extracting, scanning and burning protected health information to media, and distributing the media. This could also include the time spent preparing an explanation or summary of the protected health information, if appropriate.
- A Covered Entity may not charge a retrieval fee, whether a standard retrieval fee or one based on actual retrieval costs.
- Fees associated with maintaining systems and recouping capital for data access, storage and infrastructure are not considered reasonable, cost-based fees, and may not be included.
- Covered Entities are not required to obtain new types of technology needed to comply with specific individual requests, and therefore the cost of obtaining such new technologies is not a permissible fee to include in supply costs.
- A Covered Entity is permitted to charge for postage if an individual requests that it transmit portable media containing an electronic copy through mail or a courier (e.g., if the individual requests that the Covered Entity save PHI to a CD and then mail the CD to the individual).
- The fee limitations imposed under HIPAA apply only to an individual's request for access to their own records—it does not apply to an individual's request to transmit records to a third party. While the HITECH Act grants individuals the right to obtain a copy of their PHI maintained electronically and if the individual chooses, to direct the Covered Entity to transmit such copy directly to an entity or person designated by the individual (e.g., an attorney), such requests are not subject to HIPAA's fee limitations, but are still subject to the Michigan Medical Record Access Act fee limitations, as well the Information Blocking Rules.

The Information Blocking Final Rules clarify that charging a fee for copies of electronic PHI in a manner consistent with HIPAA does not generally constitute Information Blocking.

SHUTTERSTOCK: METAMORWORKS

THE SECURITY RULE

3

Unlike the HIPAA Privacy Rule (which applies to written, spoken and electronic PHI, the HIPAA Security Rule applies only to electronic PHI.

The Security Rule requires physicians maintaining PHI in an electronic format to implement administrative, physical and technical safeguards for protected electronic PHI, including:

- Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
- Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- Protect against reasonably anticipated, impermissible uses or disclosures; and
- Ensure compliance by their workforce.

Administrative Safeguards consist of administrative functions taken to select, implement and maintain security measures to protect electronic PHI (e.g., performing a risk analysis, naming a security official, and adding security terms to Business Associate agreements).

Physical Safeguards are steps you must take to protect your electronic information systems, equipment and your physician office space from unauthorized access and from natural or environmental hazards (e.g., implementing controls that limit physical access to authorized personnel and taking steps to secure your computer work stations).

Technical Safeguards are those automated processes that are used to protect and control access to electronic PHI (e.g., structuring your information systems with strict password protections so that only authorized persons or software programs are granted access, having mechanisms to audit and examine your information system activity for improper access, having policies to protect information from improper alteration or destruction, etc.). The use of encryption for your electronic Protected Health Information is not mandatory.

When drafting the Security Rule, HHS took a “goal oriented” approach instead of attempting to come up with a specific list of required actions that physicians must take to comply with the Security Rule. The goal was to develop the general Administrative, Physical and Technical Safeguards protecting the confidentiality, integrity and availability of electronic PHI. The advantage to this approach is the flexibility afforded to large versus small, complex versus simple health care environments when complying with the Security Rule. The disadvantage is the lack of clear guidance as to what exactly must be done (unlike the Privacy Rule, which contains, for the most part, very specific guidance) to comply with the Security Rule and the resulting lack of assurance that you have done all that is required.

However, the Security Rule does contain a series of Implementation Specifications, which are instructions on how to go about implementing the Administrative, Technical and Physical Safeguards that are required to be put into place. Each of these Implementation Specifications has been designated as either "required" or "addressable." Required specifications are mandatory for all Covered Entities and Business Associates and must be implemented. Addressable specifications are suggested methods of compliance that you must evaluate in light of your risk analysis, existing security measures, financial resources, etc. For this purpose, consideration must be given to:

- your size, complexity and capabilities;
- your technical, hardware and software infrastructure;
- the cost of such security measures; and
- the likelihood and possible impact of potential risks to your electronic PHI.

If you determine that, after an appropriate evaluation, an Implementation Specification is not a reasonable and appropriate safeguard, you do not have to implement it. The fact that the evaluation was conducted and the facts used to make the determination that an Implementation Specification was not reasonable and appropriate must be documented or you will be deemed to not have complied with the Security Rule.

A detailed discussion of each of the Implementation Specifications is beyond the scope of this Guide. **A checklist of these Implementation Specifications (Form 6) is available for your use at msms.org/HIPAASampleForms.** Physicians should complete this checklist and in any instance where an addressable specification has not been implemented, an attachment to the checklist should be created documenting the date of the evaluation of the specification and the reason(s) why the standard was not deemed to be reasonable and appropriate.

SHUTTERSTOCK: ST_TRAVEL

WHAT TO DO IF A BREACH OCCURS 4

The Privacy Rule contained a provision obligating you to mitigate, to the extent practicable, any harmful effect that is known to have occurred as a result of a wrongful disclosure of PHI either by your practice or a Business Associate. However, the exact response required following a wrongful disclosure was not specified.

Under the HITECH Act Breach Notification Rule, the discovery of a "breach" of "unsecured" PHI triggers an obligation by the Covered Entity to notify the affected individuals and requires Business Associates to notify the physician practice or other Covered Entity with which they have contracted. PHI is "unsecured" if it is not secured through the use of an HHS-specified technology or methodology that renders it unusable, unreadable, or indecipherable to unauthorized individuals.

The Breach Notification Rule defines a "breach" as the acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule which compromises the security or privacy of such information. 45 CFR §164.402. Exceptions to the definition of breach are provided for situations involving (1) any unintentional acquisition, access, or use of PHI by a member of your workforce in good faith and within the scope of authority, provided it does not result in further use or disclosure in a manner not permitted under the Privacy Rule; (2) where an inadvertent disclosure occurs by an individual who is authorized to access PHI within your practice (or one of your Business Associates) to another similarly situated individual in your practice (or the same Business Associate), as long as the PHI is not further required, accessed, used or disclosed without authorization; and (3) a disclosure of PHI where a you or your Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

The Omnibus Final Rule clarifies that an impermissible use or disclosure of PHI is presumed to be a "breach," unless an exception applies or the Covered Entity or Business Associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

- the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- the authorized person who used the PHI or to whom the disclosure is made;
- whether the PHI was actually acquired or reviewed; and
- the extent to which the risk to the PHI has been mitigated.

When a breach occurs, a Covered Entity must undertake and document a risk assessment based on (at a minimum) the above factors to determine the probability that the PHI has been compromised.

A breach is treated as discovered as of the first day on which it is known by you or your Business Associate, or, if by exercising reasonable diligence, would have been known to you or your Business Associate. You are deemed to have knowledge of a breach if it is known, or by exercising reasonable diligence would have been known.

Following discovery of a breach of PHI (whether discovered by you or after being informed of a breach by your Business Associate), you must notify each individual whose unsecured PHI has been, or is reasonably believed to have been, inappropriately accessed, acquired, or disclosed in the breach. The Breach Notification Rule requires the notifications to be made without unreasonable delay, but no later than 60 calendar days after the breach is discovered. However, if a law enforcement official states to a Covered Entity or Business Associate that notification would impede a criminal investigation or cause damage to national security, the Covered Entity or Business Associate must delay notification until the time specified by the official (if the statement is made in writing) or if the statement is made orally, no longer than 30 days from the date of the oral statement (unless a written statement is thereafter submitted by the official during that time).

Written notice to the individual, or next of kin if the individual is deceased, may be made at the last known address by first class mail or by e-mail if specified by the individual. If the contact information for 10 or more individuals is insufficient or out-of-date, a substitute notice must be furnished by either posting the notice on your website home page or providing the notice in major print or broadcast media where the affected individuals

SHUTTERSTOCK: ST_TRAVEL

likely reside. If there is insufficient or out-of-date contact information for fewer than 10 individuals, a substitute notice by an alternative form of written, telephone, or other means may be provided. In cases that you deem urgent based on possible imminent misuse of unsecured PHI, notice by telephone or other method is permitted, in addition to, but not in lieu of, the above methods. Also permitted is notice to prominent media outlets within the state if a breach affects, or is reasonably believed to affect, more than 500 residents of the state.

The notification of a breach must include:

- a brief description of what happened, including the date of the breach and date of discovery, if known;
- a description of the types of PHI involved in the breach (e.g., full name, social security number, date of birth, home address, account number, or disability code);
- the steps individuals should take to protect themselves from potential harm resulting from the breach;
- a brief description of what you are doing to investigate the breach, to mitigate losses, and to protect against any further breaches; and
- contact procedures for individuals to ask questions or to learn additional information, which must include a toll free telephone number, an e-mail address, website, or postal address.

For breaches of unsecured PHI involving 500 or more individuals, you must (except in cases involving law enforcement delay) notify HHS contemporaneously with the notice to the affected individuals. For breaches of unsecured PHI involving fewer than 500 individuals, you must maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide notification to HHS for breaches occurring during the preceding calendar year, in the manner specified on the HHS Website. HHS must annually prepare and submit to Congress a report regarding breaches for which HHS was notified.

Even when the HITECH Act Breach Notification Rule does not apply because the safe harbor for PHI that was rendered unusable, unreadable or indecipherable applies, you must still comply with other federal and state statutory and regulatory obligations that may be triggered by the breach of PHI, such as any applicable state breach notification requirements. Michigan's Identity Theft Protection Act ("ITPA") imposes notice requirements on a person who owns or licenses data included in a database that discovers a security breach. Civil fines are imposed for noncompliance with ITPA. Generally, a person is in compliance with ITPA, if that person is subject to and compliant with the Privacy Rule/HITECH Act.

The following are steps suggested to be followed in the event of a breach:

1

Determine and document whether the PHI at issue is secured or unsecured (i.e., is the breached PHI electronic and, if so, has it been rendered unusable, unreadable or indecipherable). If secured, the Breach Notification provisions do not apply.

2

If the PHI is unsecured, determine and document how many patients' PHI has been accessed, acquired, or disclosed, the circumstances, and whether it was in electronic or paper form.

3

If the PHI is unsecured, determine whether the access, acquisition or disclosure falls within one of the available exceptions. The exceptions are potentially broad enough to cover most unintentional acts such as misdirected facsimiles or e-mails, misfiled paper records, or electronic records accessed due to a mistyped search. To rely on an exception, the entity must document its assessment. If the breach falls into an exception, the Breach Notification Rule is not triggered, although obligation to mitigate harmful effects continues.

4

If the PHI is unsecured and none of the breach exceptions apply, document a risk-based assessment to determine the probability that the PHI has been compromise. If the probability is low, then the Breach Notification Rule is not triggered. If the probability is not low, then the Breach Notification Rule is triggered.

5

If the Breach Notification Rule is triggered, then furnish the required breach notification to the affected individuals and the required reports, as applicable, to HHS.

PENALTIES/ENFORCEMENT

5

The HITECH Act increased the civil monetary penalties for Privacy Rule and Security Rule violations. The penalties are arranged in four tiers (see the table on page 27), which apply based on whether or not you had knowledge of the breach, whether the breach was due to willful neglect, and when and how soon the corrective action was taken. In 2019, HHS issued a Notification of Enforcement Discretion Regarding HIPAA Civil Monetary Penalties, stating that HHS would exercise its discretion and apply a different annual civil monetary penalty limit for each of the four penalty tiers, which would be adjusted annually for inflation.

The HITECH Act also significantly expanded potential enforcement by granting enforcement authority to state attorneys general for Privacy Rule and Security Rule violations. State attorneys general can bring actions seeking injunctive relief and statutory damages equal to $100 per violation not to exceed $25,000 for all similar violations in a calendar year. Notice of any state action must be sent to HHS, which has the right to intervene.

HIPAA provides an affirmative defense to a Covered Entity against the imposition of civil money penalties for a violation of HIPAA if the violation is not due to willful neglect, and was

corrected within 30 days from the first date the Covered Entity knew or should have known the violation occurred (or within such additional period of time as determined appropriate by HHS based on the nature and extent of the violation).

Patients do not have a separate cause of action to assert claims against physicians and other Covered Entities for violations of HIPAA but may be able to assert other claims under applicable state law depending on the facts and circumstances at issue (e.g., invasion of privacy claim for improper access, use or disclosure of protected health information, complaint to state licensing board).

Congress amended the HITECH Act on January 5, 2021. The amendment requires HHS to take the existence of certain security practices into account when contemplating penalties for Covered Entities and Business Associates. Specifically, HHS is required to consider whether the Covered Entity or Business Associate is able to adequately demonstrate that it had "recognized security practices" in place for not less than the previous 12 months. If the Covered Entity or Business Associate can do so, the Covered Entity or Business Associate may benefit from reduced enforcement penalties such as early, favorable termination of an audit or reduced fines.

The amendment defines "recognized security practices" as follows:

1. the standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the National Institute of Standards and Technology Act;
2. the approaches promulgated under section 405(d) of the Cybersecurity Act of 2015; and
3. other programs and processes that address cybersecurity and that are developed, recognized, or promulgated through regulations under other statutory authorities.

The amendment does not mandate the adoption of any particular recognized security practices and expressly allows Covered Entities and Business Associates to decide what security practices are properly suited for their organizations consistent with the Security Rule.

Civil monetary penalties for Privacy Rule and Security Rule violations under the HITECH Act

Violation	Minimum Penalty	Minimum Penalty	Annual Limit *For all violations of an identical requirement prohibition.*
The person did not know and by exercising reasonable diligence would not have known that he/she violated HIPAA	$100 per violation	$50,000 per violation	**Under HITECH Act: $1.5 million** **Under 2019 HHS Enforcement Discretion:** $25,000
HIPAA violation due to reasonable cause and not due to willful neglect	$1,000 per violation	$50,000 per violation	**Under HITECH Act:** $1.5 million **Under 2019 HHS Enforcement Discretion:** $100,000
HIPAA violation due to willful neglect but corrected within the required time period	$10,000 per violation	$50,000 per violation	**Under HITECH Act:** $1.5 million **Under 2019 HHS Enforcement Discretion:** $25,000
HIPAA violation due to willful neglect and not corrected	$50,000 per violation	$50,000 per violation	**Under HITECH Act:** $1.5 million **Under 2019 HHS Enforcement Discretion:** $25,000

NOTE REGARDING FORMS

The sample HIPAA Sample Forms referenced throughout this booklet are available at msms.org/HIPAASampleForms.

The forms and suggested language listed below are intended to provide physicians with examples of what is required by the Privacy Rule and/or the HITECH Act. The exact forms used, the content of the forms, and the appropriateness of the suggested language will vary from physician practice to physician practice.

Use of these forms and the suggested language are not intended to replace the need for physicians to consult with a health care attorney with HIPAA experience for assistance in ensuring that their practice complies with all the necessary requirements.

Sample forms available include:

Form 1 ..... Sample Physician Office HIPAA Notice of Privacy Practice

Form 2..... Sample Acknowledgment of Receipt of Notice of Privacy Practices

Form 3..... Sample Authorization Form

Form 4 ..... Sample Business Associate Agreement Provisions

Form 5..... Compliance Plan Provisions

Form 6 ..... Checklist to Comply with HIPAA Security Rule

MSMS
MICHIGAN STATE MEDICAL SOCIETY

This publication is furnished for informational purposes only and may not be construed or relied upon as legal advice.

Copyright ©2026
Michigan State Medical Society and
Kerr, Russell and Weber, PLC.

MSMS
MICHIGAN STATE MEDICAL SOCIETY

Michigan State Medical Society
PO Box 23, East Lansing, MI 48823
(517) 337-1351

msms.org