

HIPAA REQUIREMENTS AND INFORMATION

HIPAA (The Health Insurance Portability and Accountability Act)

Molina Healthcare's Commitment to Patient Privacy

Protecting the privacy of members' personal health information is a core responsibility that Molina Healthcare takes very seriously. Molina Healthcare is committed to complying with all federal and state laws regarding the privacy and security of members' protected health information (PHI).

Provider/Practitioner Responsibilities

Molina Healthcare expects that its contracted Providers/Practitioners will respect the privacy of Molina Healthcare members and comply with all applicable laws and regulations regarding the privacy of patient and member PHI.

Applicable Laws

Providers/Practitioners must understand all state and federal healthcare privacy laws applicable to their practice and organization. Currently, there is no comprehensive regulatory framework that protects all health information in the United States; instead there is a patchwork of laws that Providers/Practitioners must comply with. In general, most healthcare Providers/Practitioners are subject to various laws and regulations pertaining to privacy of health information including, without limitation, the following:

1. Federal Laws and Regulations
 - HIPAA
 - Medicare and Medicaid laws
2. Applicable Washington Laws and Regulations

Providers/Practitioners should be aware that HIPAA provides a floor for patient privacy but that state laws should be followed in certain situations, especially if the state law is more stringent than HIPAA. Providers/Practitioners should consult with their own legal counsel to address their specific situation.

Uses and Disclosures of PHI

Member and patient PHI should only be used or disclosed as permitted or required by applicable law. Under HIPAA, a Provider/Practitioner may use and disclose PHI for their own treatment, payment, and healthcare operations activities (TPO) without the consent or authorization of the patient who is the subject of the PHI. Uses and disclosures for TPO apply not only to the Provider/Practitioner's own TPO activities, but also for the TPO of another covered entity¹ Disclosure of PHI by one covered entity to another covered entity, or healthcare provider, for the recipient's TPO is specifically permitted under HIPAA in the following situations:

¹See, Sections 164.506(c) (2) & (3) of the HIPAA Privacy Rule.

1. A covered entity may disclose PHI to another covered entity or a healthcare provider for the payment activities of the recipient. Please note that “payment” is a defined term under the HIPAA Privacy Rule that includes, without limitation, utilization review activities, such as preauthorization of services, concurrent review, and retrospective review of “services.”²
2. A covered entity may disclose PHI to another covered entity for the health care operations activities of the covered entity that receives the PHI, if each covered entity either has or had a relationship with the individual who is the subject of the PHI being requested, the PHI pertains to such relationship, and the disclosure is for the following health care operations activities:
 - Quality improvement
 - Disease management;
 - Case management and care coordination;
 - Training Programs;
 - Accreditation, licensing, and credentialing

Importantly, this allows Providers/Practitioners to share PHI with Molina Healthcare for our healthcare operations activities, such as HEDIS and quality improvement.

Written Authorizations

Uses and disclosures of PHI that are not permitted or required under applicable law require the valid written authorization of the patient. Authorizations should meet the requirements of HIPAA and applicable state law. A sample Authorization for the Use and Disclosure of Protected Health Information is included at the end of this section.

Patient Rights

Patients are afforded various rights under HIPAA. Molina Healthcare Providers/Practitioners must allow patients to exercise any of the below-listed rights that apply to the Provider/Practitioner’s practice:

1. Notice of Privacy Practices

Providers/Practitioners that are covered under HIPAA and that have a direct treatment relationship with the patient should provide patients with a notice of privacy practices that explains the patient’s privacy rights and the process the patient should follow to exercise those rights. The Provider/Practitioner should obtain a written acknowledgment that the patient received the notice of privacy practices.

2. Requests for Restrictions on Uses and Disclosures of PHI

Patients may request that a healthcare Provider/Practitioner restrict its uses and disclosures of PHI. The Provider/Practitioner is not required to agree to any such request for restrictions.

3. Requests for Confidential Communications

Patients may request that a healthcare Provider/Practitioner communicate PHI by alternative means or at alternative locations. Providers/Practitioners must accommodate reasonable requests by the patient.

²See the definition of Payment, Section 164.501 of the HIPAA Privacy Rule

4. *Requests for Patient Access to PHI*

Patients have a right to access their own PHI within a Provider/Practitioner's designated record set. Personal representatives of patients have the right to access the PHI of the subject patient. The designated record set of a Provider/Practitioner includes the patient's medical record, as well as billing and other records used to make decisions about the member's care or payment for care.

5. *Request to Amend PHI*

Patients have a right to request that the Provider/Practitioner amend information in their designated record set.

6. *Request Accounting of PHI Disclosures*

Patients may request an accounting of disclosures of PHI made by the Provider/Practitioner during the preceding six (6) year period. The list of disclosures does not need to include disclosures made for treatment, payment, or healthcare operations or made prior to April 14, 2003.

HIPAA Security

Providers/Practitioners should implement and maintain reasonable and appropriate safeguards to protect the confidentiality, availability, and integrity of member PHI. Providers/Practitioners should recognize that identity theft is a rapidly growing problem and that their patients trust them to keep their most sensitive information private and confidential.

In addition, medical identity theft is an emerging threat in the healthcare industry. Medical identity theft occurs when someone uses a person's name and sometimes other parts of their identity—such as health insurance information—without the person's knowledge or consent to obtain healthcare services or goods. Medical identity theft frequently results in erroneous entries being put into existing medical records. Providers should be aware of this growing problem and report any suspected fraud to Molina Healthcare.

HIPAA Transactions and Code Sets

Molina Healthcare strongly supports the use of electronic transactions to streamline healthcare administrative activities. Molina Healthcare Providers/Practitioners are encouraged to submit claims and other transactions to Molina Healthcare using electronic formats. Certain electronic transactions are subject to HIPAA's Transactions and Code Sets Rule including, but not limited to, the following:

- Claims and encounters
- Member eligibility status inquiries and responses
- Claims status inquiries and responses
- Authorization requests and responses
- Remittance advices

Molina Healthcare is committed to complying with all HIPAA Transaction and Code Sets standard requirements. Providers/Practitioners who wish to conduct HIPAA standard transactions with Molina

Healthcare should refer to Molina Healthcare's website at <http://www.molinahealthcare.com> for additional information. Click on the tab titled "Providers", select a state, click the tab titled "HIPAA" and then click on the tab titled "TCS readiness".

National Provider Identifier

Provider/Practitioners must comply with the National Provider Identifier (NPI) Rule promulgated under HIPAA. The Provider/Practitioners must obtain an NPI from the National Plan and Provider Enumeration System (NPPES) for itself or for any subparts of the Provider/Practitioner. The Provider/Practitioner must report its NPI and any subparts to Molina Healthcare and to any other entity that requires it. Any changes in its NPI or subparts information must be reported to NPPES within 30 days and should also be reported to Molina Healthcare within 30 days of the change. Provider/Practitioners must use its NPI to identify it on all electronic transactions required under HIPAA and on all claims and encounters (both electronic and paper formats) submitted to Molina Healthcare.

Additional Requirements for Delegated Providers/Practitioners

Providers/Practitioners that are delegated for claims and utilization management activities are the "business associates" of Molina Healthcare. Under HIPAA, Molina Healthcare must obtain contractual assurances from all business associates that they will safeguard member PHI. Delegated Providers/Practitioners must agree to various contractual provisions required under HIPAA's Privacy and Security Rules.