

	<b>Ethics &amp; Compliance Department</b>	
	<b>Policy No.: 53</b>	<b>Created:</b> 01/2018
		<b>Reviewed:</b> 06/2025
		<b>Revised:</b> 06/2025

## **HIPAA: APPROPRIATE ACCESS**

### **SCOPE:**

All Envision Healthcare teammates. For purposes of this policy, all references to “teammate” or “teammates” include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

### **PURPOSE:**

Envision Healthcare Operating, Inc. and its subsidiaries and affiliates (“Envision” or “the Company”) has adopted this Appropriate Access policy to define appropriate access levels to the medical record and all related protected health information (“PHI”).

### **POLICY:**

Access to PHI in the possession of or under the control of the Company must be determined and provided based on the need to access such information directly related to a teammate’s duties and responsibilities. Accordingly, the Company has established access controls that will restrict access to health information to those employees who have a business need to access it.

Company teammates who are also patients are required to comply with the same policies and follow the same procedures as all other patients related to accessing and amending their medical record. Teammates may *not* use the privileges associated with their position to view their own medical records or related PHI, including billing records, or the records of family or friends.

Business associates will be given access to PHI and/or PHI will be disclosed to them only when there is a legitimate business need for the information and a Business Associate Agreement has been executed.

Teammates and business associates must not attempt to access PHI unless they have been granted appropriate access rights and have a clear business reason to do so. Each owner of a specific portion of information must determine which teammates by position and/or responsibility should be given access to such information. Further, the owner is to determine the level of access, including the right to view, amend or include information, or deny access to PHI in its entirety. Questions concerning appropriate access can be directed to the Company’s Privacy Official.

While the Medical Records Department at each facility of the Company or Company’s various facility contracts is the true custodian of the medical record, all office-based records are “owned” by the Company. Further, all related billing information, record copies, and other such data delivered or submitted to the corporate offices or other locations for billing purposes is “owned”

	<b>Ethics &amp; Compliance Department</b>	
	<b>Policy No.: 53</b>	<b>Created:</b> 01/2018
		<b>Reviewed:</b> 06/2025
		<b>Revised:</b> 06/2025

by the Company. It is the responsibility of the department who generates or warehouses specific information to determine the access rights and security of the information.

### **Remote Access**

All remote access connections associated with the Company's computer systems must be established within the guidelines of the Company's information technology security policies. All teammates requiring remote access must comply with established privacy and security policies. No remote connections will be established without the authorization of the Information Technology Department.

### **POLICY REVIEW**

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.