



Virtual Integrated Patient Record (VIPR) Privacy & Security

Great Lakes Health Connect values your partnership in building care-connected communities. Together we strive to improve health outcomes and healthcare value for patients, providers, and payers across Michigan and beyond. In achieving this goal, protecting patient health information must be a top priority.

To honor the privacy commitments we all make to patients, please remember:

- Patient information is confidential and it is your responsibility to protect it. Information available via VIPR may only be accessed, used, and disclosed as permitted by law and all other applicable regulations, including, but not limited to, HIPAA, 42 CFR Part 2, and applicable state law.
- VIPR is for authorized use ONLY. Do not access more information than necessary to complete your duties.
- Even if you are a legal guardian or authorized representative of an individual, please refrain from using VIPR to access their medical information.
- Use of your password and username by anyone other than you is strictly prohibited. Your username and password acts as a "signature". You are accountable for all actions taken using your username and password.
- You are required to change your password on a periodic basis. Choose a strong password. If you suspect someone other than you is in possession of your password, please change it immediately and contact GLHC support.
- Ensure the computer you use to access VIPR is protected against viruses and other malicious code. Updated anti-virus software and other protections should always be enabled.
- Please report any suspected or confirmed breach of information accessed in VIPR to the GLHC Privacy Officer immediately. Also report any known security threats that might affect GLHC.
- You are responsible for managing and monitoring all decisions and actions taken or not taken involving patient care, utilization management, and quality management resulting from or in any way related to the use of data or information provided by or through GLHC.
- All activity in VIPR is logged and monitored. Any suspected improper access or use is reported to Management at your organization.