


# Policy & Procedure

<p><b>POLICY/PROCEDURE TITLE:</b> Provider Network Documentation and Electronic Medical Record Use</p> <p><b>POLICY/PROCEDURE #:</b> 713</p> <p><b>Section:</b> Provider Network</p> <p><b>Developed and maintained by:</b> Provider Network Manager</p> <p><b>Scope:</b> <input type="checkbox"/> OnPoint Staff <input type="checkbox"/> MH/IDD, <input type="checkbox"/> Housing, <input type="checkbox"/> SUD, <input type="checkbox"/> Integrated Health, <input checked="" type="checkbox"/> OnPoint Contract Providers  <input type="checkbox"/> Other _____</p>	<p><b>Approved By:</b>           (Chief Executive Officer)</p> <p><b>Approved By:</b> _____          (Medical Director; as applicable)</p>	
	<b>DATES</b>	
	<b>First Effective</b>	4/1/25
	<b>Revised</b>	N/A
	<b>Reviewed</b>	4/1/25

**PURPOSE** To establish clear and consistent expectations for the use of electronic medical records (EMR) to document services delivered within the OnPoint Provider Network, and to describe a standardized procedure for accessing and utilizing OnPoint’s EMR.

**POLICY**

1. OnPoint strongly encourages the use of Electronic Medical Record (EMR) systems to maintain client information, document and store records of service delivery, and facilitate the performance of required reporting. Such EMR systems advance OnPoint’s mission and operational sustainability by increasing efficiency, improving the quality and completeness of documentation, and ensuring fulfillment of applicable requirements.
2. Users of the OnPoint EMR shall adhere to all applicable laws, regulations, and policies/procedures.
3. All provider agency staff must request and be granted access by OnPoint EMR System Administrators prior to accessing and/or using OnPoint’s EMR (see procedure below for how to request access).
4. OnPoint may limit, suspend, or revoke any user’s access to the OnPoint electronic medical record at any time. Inappropriate use may subject a user to legal proceedings or criminal charges, and/or contract termination.
5. When provider agency staff leave their employer, provider agencies shall promptly notify OnPoint EMR System Administrators of the separation, so that the account can be deactivated and unauthorized access is prevented.
6. If external provider accounts have no activity within 45 days, the account will be automatically disabled and can only be accessed by requesting reactivation by OnPoint EMR System Administrators.

## Policy & Procedure

7. Any information composed, stored, sent, or received using the OnPoint electronic medical record system is the property of OnPoint. OnPoint reserves the right to monitor and use the data as deemed necessary.
8. OnPoint will not be held liable for data breach occurring at the Provider level.
9. External Providers will complete an External Provider EMR Attestation to identify their intended usage of electronic medical records for service documentation. Attestation shall be completed at the time of initial or renewal of the provider contract.
10. Documentation, regardless of method, shall meet all requirements as identified in OnPoint Policy 442-Service Documentation, Authentication of Services and Billing.
11. Staff shall uphold strong security standards by utilizing the following measures. The list of standards provided is not exhaustive.
  - a) Maintain confidential records
  - b) Select strong passwords
  - c) Inform OnPoint of separation of employees within 5 business days of employment termination.
  - d) Log out when not in use
  - e) All staff who will have access to the EMR shall have annual cyber security training

### PROCEDURES

1. Provider Requests to Access OnPoint EMR:
  - a) Providers shall submit requests for access to the OnPoint EMR identifying staff names, roles and type of access requested.
  - b) Requests shall be sent to OnPoint by Provider Leadership.
2. Setting Provider Staff User Permissions
  - a) To ensure data integrity and to protect the confidentiality of protected health information (PHI), OnPoint shall assign user permissions at the lowest level necessary for users to complete their work.
  - b) Lower Level of Care SUD providers who deliver outpatient level SUD services will have the ability to add clients to OnPoint's EMR. This function is necessary for providers to be able to deliver same-day access/walk-ins.
  - c) To limit the risks involved with allowing external users create new clients in the OnPoint EMR, OnPoint shall limit the number of provider agency staff to three (3) or less per organization, who have OnPoint Provider Network Manager will direct which provider agencies may have "Add Client" permission. Exceptions may be made on an individualized basis through consultation with EMR System Administrators and OnPoint Provider Network Manager.
  - d) Coordination and consultation with the Provider Network team will occur is questions arise regarding the number of staff who can add clients in OnPoint's EMR.

## Policy & Procedure

3. At the time of initial contract execution, and during each contract renewal cycle thereafter, subcontracted external providers must select a method for documenting service delivery from the following options:
  - a) **Utilize an Electronic Medical Record of the provider's choosing.**
    - i. Providers may choose to implement and maintain their own EMR.
    - ii. Provider shall upload service documentation to OnPoint's Electronic Medical record prior to submitting the claim.
  - b) **Elect to utilize OnPoint's Electronic Medical Record.**
    - i. Providers that are unable to obtain their own EMR may opt to utilize OnPoint's EMR for clinical/service delivery documentation.
    - ii. Providers may be charged a minimal fee to utilize OnPoint's EMR, which will be identified in the provider service contract and deducted from provider payment.
  - c) **Submit a request for a waiver to use an alternative method of documenting service delivery.**
    - i. Waivers may be considered for providers serving less than three individuals.
    - ii. Providers delivering services such as Respite Camps, Recovery Residences, etc. may be eligible for a waiver. This is not an inclusive list of service types however service type may be a consideration during the review process.
    - iii. The OnPoint Chief Administrative Officer, or designee, will review and make a determination of the appropriateness of granting a waiver.
    - iv. Disputes regarding EMR waiver determinations may be appealed to the OnPoint Chief Executive Officer (CEO).
4. Cyber Security Insurance
  - a) OnPoint recommends that providers have at a minimum of \$500,000 cyber security insurance coverage.
  - b) Any provider receiving grant funding is required to have \$1,000,000 each occurrence and \$1,000,000 annual aggregate cyber security insurance coverage, which will be specified in the contract. Coverage must include information security and privacy liability, privacy notification costs, regulatory defense and penalties, and website media content liability. OnPoint may request an exemption from the PIHP, if the provider is determined low risk related to cyber security.
5. Oversight and Monitoring
  - a) Auditing/Monitoring will take place to ensure providers are utilizing the EMR as intended.
  - b) Reports will be run to ensure staff access is accurate and up to date.
  - c) System Administrators will monitor system use and the number of provider staff with assigned permissions for existing providers and will adjust permissions accordingly.

## **Policy & Procedure**

### **REFERENCES**

- PIHP/CMHSP Contract
- OnPoint Policy 442-Service Documentation, Authentication of Services and Billing.

### **ATTACHMENT(S)**

- 713.1 Provider Network Electronic Medical Record Attestation
- 713.2 Provider Network Electronic Medical Record Waiver Request
- 713.3 Provider Network Request for access to OnPoint EMR