|  |  |
| --- | --- |
| **ORGANIZATIONS:**  Map to Health, LLC DBA Recovery Unplugged  Recovery Unplugged Austin, LLC  Recovery Unplugged Encore, LLC  Recovery Unplugged Northern Virginia  Recovery Unplugged Nashville, LLC | **POLICY TITLE:**  Health Insurance Portability and Accountability (HIPAA) and Confidentiality |
| **EFFECTIVE DATE:**  8/1/19 | **POLICY NUMBER:**  OP-IM-4.00 |
| **DEPARTMENT/PRIORITY:**  All Departments | **REVISION DATE(S):**  4/15/2020, 8/19/2020 |
| **JOINT COMMISSION STANDARD:**  IM.02.01.01; IM.02.01.03; RI.01.01.01, EP 7 | **LEGAL REFERENCE:**  FL- 65D-30.004(12), (28)  TX- 448.508  VA- 12VAC35-105- 870(B)  TN- 0940-05-06-.02(1)(f) |

**POLICY:**

Recovery Unplugged ensures that all personnel, contractors, management and executives comply with the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Federal Law of Confidentiality as stated 42CFR Part 2. All levels of care are covered by the HIPAA and Federal Law of Confidentiality and as such must be in compliance with all of the applicable tenets of the Act.

**PROCEDURE:**

1. Employees take a HIPAA training upon hire and annually, as well as sign a Confidentiality and Non-Disclosure Agreement upon hire that will be placed in their employee file.
2. Employees must have an assigned username and password to be granted access to any desktop computer. The access will only be granted for their specific desktop and employees will not be granted access to other employee’s desktops.
3. Recovery Unplugged uses an Electronic Medical Records system (EMR) called Kipu. Kipu has implemented measures to ensure the safety of HIPAA protected files including:
   1. Built for the cloud; no VPN or other applications required
   2. Data encryption and HIPAA certified by MBHC
   3. Separate virtual servers for each client
   4. Servers are on a private network, not just exposed for hackers to see
   5. NOT multi-tenant or multi-user
   6. Regular data intrusion testing
   7. Two-Factor authentication
4. The use and disclosure of protected health information (PHI) falls into three (3) basic categories under HIPAA and each are must be addressed separately.
   1. Required: Uses and disclosures that must be made to comply with the law and are not subject to consent or authorization by Recovery Unplugged.
   2. Permitted: Uses and disclosures that are allowed under the law, but not required, and are not subject to consent or authorization by Recovery Unplugged.
   3. Restricted: Uses and disclosures that are not allowed without the consent or authorization of Recovery Unplugged.
5. Limits of confidentiality include:
   1. Client must consent in writing
   2. Disclosure is allowed by court order
   3. Disclosure to medical personnel in case of emergency
   4. Disclosure for healthcare operations
   5. Disclosure if client is a danger/threat to themselves or others
   6. Disclosure to qualified professionals for research/audit
   7. Disclosure if crime is committed on premises or against personnel
   8. Disclosure due to suspected child/elderly abuse/neglect
6. Recovery Unplugged programs shall not use or disclose PHI without a valid authorization by the client, unless permitted by law or if the situation falls into the limits of confidentiality. All such uses and disclosures shall be consistent with the valid authorization and applicable law. Recovery Unplugged has each client sign a Release of Authorization form upon intake or whenever PHI is going to be disclosed. (See attachment 4.00(a))
   1. All Medical Records requests shall be submitted to the Medical Records Department via department email. Staff shall not release Medical Records.
   2. The submission request shall include documents being requested, reason and ROI, if necessary.
   3. Recovery Unplugged has thirty (30) days to provide the medical record once the request has been received.
   4. Recovery Unplugged may deny access to any portion of the record if determined that release of that portion would be harmful to the client or other’s physical, mental, or emotional health according to state and federal law.
7. All client information, counseling sessions, and records shall be kept confidential.
8. Recovery Unplugged contracts with outside personnel, who may have access to PHI. Those personnel sign a Business Associate Agreement and/or Confidentiality and Non-Disclosure Agreement that states federal regulations regarding HIPAA and confidentiality.
9. Please see policy OP-CL-7.02 for additional policies on Confidentiality.