RCIT-803

TITLE: Privacy of Client Information Confidentiality

EFFECTIVE DATE: 2/16/21 AUTHORIZED BY: Board of Trustees

ODMHAS 5122:27-11

Confidentiality

Notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please review it carefully.
If you have any questions about this notice please contact:

Lesley Stegall, Clinical Director. Phone:937-403-9108 Address: 910 South St, Greenfield, OH 45123 E-mail: lesleys@reach4t.org

OUR DUTIES

At REACH For Tomorrow Inc , we are committed to protecting your health information and safeguarding this information against unauthorized use or disclosure. This Notice will tell you how we use and disclose your health information. It also describes your rights and the obligations we have regarding the use of disclosure of your health information. We are required by law: 1)Maintain the privacy of your health information. 2) Provide you notice of our legal duties and privacy practices with respect to your health information. 3) to abide by the terms of the notice that is currently in effect; and 4) to notify you if there is a breach of your unsecured health information.

HOW WE ME USE AND DISCLOSE YOUR PERSONAL HEALTH INFORMATION
When you receive Services paid in full or part by Medicaid, we receive health information about you. We may receive Healthcare operations, communicating with your health care providers about your treatment and for other purposes permitted or required by law.

Other Uses and Disclosures - We may also use or disclose your personal health information for the following reasons as permitted or required by applicable law: To alert proper authorities if we reasonably believe that you may be a victim of abuse, neglect, or domestic violence or other crimes; to notify public or private entities authorized by law or Charter to assist in disaster relief efforts, for the purpose of coordinating family notifications; to reduce or prevent threats to Public Health and safety; for health oversight activities such as evaluations, investigations, Audits, and inspections**;** to governmental agencies that monitor your services; For lawsuits and similar proceedings; for public health purposes such as to prevent the spread of a communicable disease; for certain approved research purposes; for law enforcement reasons if required by law or in regards to a crime or suspect; to Correctional institutions in regards to inmates; the coroners, Medical examiners and funeral directors (for decedents); as required by law; for organ and tissue donation; for specialized government functions such as military and veterans activities, national security and intelligence purposes, and protection of the President; For workers compensation purposes; for the management and coordination of public benefits programs; to respond to requests from the US Department of Health and Human Services; and for us to receive assistance from Consultants that have signed an agreement requiring them to maintain the confidentiality of your personal information. Also, if you have a guardian or power of attorney, we are permitted to provide information to your guardian or attorney of facts.

User Disclosures That Require Your Permission
You are prohibited from selling your personal information, such as to a company that wants your information in order to contact you about their services, without your written permission. We are prohibited from using or disclosing your personal information for marketing purposes, such as to promote our services, without your written permission. All other uses of your health information not described in this notice will be made only with your written permission. If you provide us with permission to use or disclose health information about you, you may revoke that permission, in writing, at any time. If you revoke your permission, we will no longer use or disclose your health information for the purposes state in your written permission except for those that we have already made prior to your revoking that permission.

Prohibited Uses and Disclosures
If we use or disclose your health information for underwriting purposes, we are prohibited from using and disclosing the genetic information in your health information for such purposes.

POTENTIAL IMPACT OF OTHER APPLICABLE LAWS
If any state or federal privacy laws require us to ride you with more privacy protections than those explain here and we must also follow that law. For example, drug and alcohol treatment records generally receive greater protections under federal law.

YOUR RIGHTS REGARDING YOUR PERSONAL HEALTH INFORMATION

You have the Following rights regarding your health information:

- Right to request restrictions. You have the right to request that we restrict the information we use or disclose about you for purposes of treatment, payment, Healthcare operations and informing individuals involved in your care about your care or payment for that care.
- Right to inspect and copy. You have the right to request access to certain health information we have about you. Fees may apply to copy information.
- Right to amend. You have the right to request Corrections or additions to certain health information we have about you. You must provide us with your reason for requesting the change.
- Right to an accounting of disclosures. You have the right to request an accounting of the disclosures we make of your health information, except for those made with your permission and those related to treatment, payment, our health care operations,, and certain other purposes. Your request must include a time frame for the accounting, which must be within 6 years prior to your request. The first accounting is free but he will apply if more than one request is made in a 12-month period.
- Ride to a paper copy of notice. You have the right to receive a paper copy of this notice.

To File a Complaint

If you believe your privacy rights have been violated, you may file a complaint with the client Advocate or with the secretary of the Department of Health and Human Services. To file a complaint with the client Advocate, contact he / she at the address above. You and I'll be retaliated against for filing a complaint. If you wish to file a complaint with the secretary you may send complaint to:

Office for civil rights
US Department of Health and Human Services
Attn: Regional manager
233 North Michigan Avenue, Suite 240
Chicago Illinois 60601

The confidentiality of all persons receiving services from REACH For Tomorrow Inc shall be protected. Any proceeding, recording, writing, data, reports, information, or any other material under the auspices of REACH For Tomorrow Inc shall be held in strict confidence and shall be appropriately safeguarded. An employee may not make copies or remove any client or REACH For Tomorrow Inc records without prior approval. A staff person's access to an individual client's records, treatment information, diagnosis or other protected information is limited to access and disclosure in accordance with all applicable federal and state laws and regulations. Storage of clients records shall be in accordance with all applicable federal and state laws and regulations. All files will be secured in a locked file room.

All professional staff are expected to abide by their professional code of ethics in accordance with their respective licensing or credentialing boards. All employees, student interns, independent contractors, and volunteers will sign the "Confidentiality Agreement" immediately upon the beginning of their duties with REACH For Tomorrow Inc. Each employee is required to review the policy on confidentiality annually. This may be accomplished when an employee receives their annual evaluation.

Any employee who violates this Confidentiality provision will be subject to immediate termination.All information disclosed is bound by the federal law and regulations Governing confidentiality of Alcohol and Drug Abuse Patient Records [42 U.S.C. 290dd-2; 42 C.F.R. Part 2]

Client Records Storage/Electronic Health Record (EHR)

Policy: Company shall store records on site in an Electronic Health Record (EHR) and in compliance with local, state and federal laws and regulations, specifically HIPAA and 42 C. F. R. part 2.

Procedure:

1. Company shall create and maintain clinical records electronically with agency-owned computers using web-based Electronic Health Records provided by BestNotes LLC and NextGen LLC, that are protected using access control tools including, but not limited to, passwords to limit access to client information to authorized individuals.
2. Written records will be maintained/stored in a secure room, locked file cabinets, safe, or other similar container when not in use.
3. Company shall password protect clinical records.
4. The company shall maintain records for a minimum of 7 years past the discharge of any client.
5. Client records shall be retained/destroyed in accordance with Ohio Administrative Code 3793:2-1-06

Client Record Security, Maintenance, and Destruction

Policy: Company shall assure that clinical records/electronic health records are recorded, collected, maintained, stored, and destroyed in a secure manner in which Protected Health Information remains confidential.

Procedures:

1. Company shall authenticate records that assures the accuracy regarding the identity of a user and the source of data is as claimed (i.e. Probation officer, other treatment provider, guardian).
2. Company shall grant rights to allow each user to access only functions, information, and privileges required by his/her duties.

3. Company shall assure integrity of the system by ensuring that information is changed only in a specific and authorized manner. Data, program system, and network integrity are all relevant to consideration of computer and system security.
4. The Company shall implement audit trails that are created immediately and concurrently with user actions that compile a chronological record of activities occurring in the system.
5. Company leadership shall assure, in consultation with EHR vendor Bestnotes LLC, that client records are stored and maintained in such a manner that minimizes the risk of record damage or loss.
6. Company leadership shall oversee, in collaboration, with its EHR vendor, Bestnotes LLC, that clinical records are stored predictably by location/server, maintained responsibility/securely, and accessed properly to exchange data as needed for legitimate program purposes.
7. Company leadership shall implement the proper use of electronic signatures. A signature code consisting of a combination of letter, numbers, characters or symbols that is adopted or executed by an individual as that individual's electronic signature; a computer-generated signature code created for an individual; or an electronic image of an individual's handwritten signature created by using a pen computer. Client record systems utilizing electronic signatures shall comply with section 3701.75 of the Ohio Revised Code.
8. The company will oversee that each user of the system must certify in writing that the user will follow the confidentiality and security policies maintained by the entity for the system. The penalties for misusing the system will clearly be stated in the written/signed agreement. There will be training for all users of the system that includes an explanation of the appropriate use of the system and the consequences for not complying with Company's confidentiality and security policies.
9. In cases of Legally valid requests, REACH For Tomorrow Inc will provide a paper copy of client records.

IT Disaster Relief Plan

1. In the event of a natural or other occurring disaster which results in loss of power to the facility and potential corruption of sensitive staff/patient information:
   Staff accounts and payroll information, client/patient demographics, insurance information, and ROI's for emergency contact, referral sources, clinical curriculum and schedule are to be included in secured storage. It is essential to maintain back-up files for all information necessary for the continuation of services at REACH for Tomorrow.

   In the event of power failure and possible corruption of files, staff on site will immediately contact the clinical manager to implement the IT disaster relief plan, to include, but not limited to, the physical retrieval of the secure backup server with files/information (BestNotes) essential for the continuation of services. Upon retrieval of the storage unit, files will be distributed back onto the appropriate devices once security has again been verified.

HIPAA Compliance Statement From BestNotes LLC
Updated April 19, 2018

BestNotes, LLC including BestNotes CRM/EMR and OutcomeTools, is fully compliant with the HIPAA Standards for Privacy, Electronic Transactions and Security (including the HITECH Act and the Omnibus Rule of 2013). BestNotes has implemented policies, processes, and procedures designed to ensure compliance with Federal and State information security laws, regulations, and rules, and monitors ongoing compliance efforts with assistance from Compliancy Group LLC. This process includes a risk analysis of administrative (policies and procedures), technical (all devices connecting to or storing ePHI, e.g. routers, firewalls, servers, workstations) and physical (paper shredding, alarm systems, and general security of each site) controls as well as disaster recovery planning.

BestNotes' recognizes that it is a key business partner with its customers and will continue to provide all of its various programs and services in accordance with the relevant requirements of all state and federal laws and regulations, including, as applicable, HIPAA.

Questions regarding BestNotes' HIPAA policies or compliance may be directed to:

BestNotes, LLC
Attention: Benjamin Elison, HIPAA Security Officer
PO Box 5578
Twin Falls, Idaho 83303-5578
team@bestnotes.com

Certain information provided to Us may be Protected Health Information as that term is defined in the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), American Recovery and Reinvestment Act ("ARRA"), Health Information Technology for Economic and Clinical Health Act ("HITECH") and in regulations promulgated there under and it may also be subject to regulation under state law ("PHI"). We offer and provide the Company Site and Our products and services in a manner that complies with all applicable laws and regulations we are aware of and/or become known to us and will continue to do so. As an example, We have Business Associates Agreements in place with Our customers, partners and vendors that govern the disclosure and use of PHI that is required for Us to provide them with the products and services they have requested.

If You order services from Us that require You to provide to Us personal health information that is protected under any federal or state laws (including HIPAA), You grant to Us a non-exclusive, perpetual, irrevocable, royalty-free right and license to use de-identified patient and administrative data ("De-Identified Use Data" as defined under 45 C.F.R. § 165.514) collected or provided through your use of the Company Site for any lawful business purpose, provided that such data is not personally identifiable. We shall have the right to de-identify such patient and administrative data and then utilize the De-Identified Use Data for any lawful purpose, including but not limited to creating statistical norms and reports de-identified score cards, regional or national benchmarking, or to be used for research considerations, provided however that the data shall not include member identities and claims information that is unprotected. A personally identifiable patient, physician and Your information shall remain confidential and shall not be released. Further, should We choose to place the De-Identified Use Data in its national database or in any way incorporate such data in studies and/or analyses conducted directly or indirectly by Us, no such data shall be identified as originating from You, or Your

patients, members, or physicians. The De-Identified Use Data shall also not be utilized in any study, report or publication without first being integrated with a significant body of other data such that neither

You or Your patients or physicians can be identified, unless appropriate, advance and written consents to such identification are obtained.

We use appropriate security measures to protect the information We obtain from unauthorized alteration, loss, disclosure, or use, including technological, physical and administrative controls over access to the systems We use to provide the Company Site and Our products and services. As an example, we restrict access to particular systems and information to those employees and independent contractors whose duties require them to have it. To obtain this access, employees and independent contractors are required to agree not to: (a) disclose that information; or (b) use their access or any confidential information except to exercise their rights or discharge their obligations under their respective agreements.

MINORS
In the case of minors (under the age of eighteen) permission to release information must be signed by the parent/legal guardian.

a. Information is only to be released when an Authorization for Release of Information form is signed by the client and/or legal guardian and witnessed by program staff.
b. All requests for information that occurs when a person is deceased will require a probate court mandate or subpoena prior to releasing any client information.
c. Federal law and regulations do not protect any information about a crime committed by a client either at the agency or against any person who works for the agency, or about any threats to commit such a crime.

HIV
If the records released include information of an HIV-related diagnosis or test result, the following statement must be added to the released information:

> This information has been disclosed to you from confidential records protected from disclosure by state law. You will make no further disclosure of this information without the specific, written, and informed release of the individual to whom it pertains, or as otherwise permitted by state law. A general authorization for the release of medical or other information is NOT sufficient for the purposes of the release of HIV test results or diagnoses.