Confidentiality Policies and Procedures

© Copyright Achieve Beyond Pediatric Therapy & Autism Services 2018

Policy on Maintaining Records

Achieve Beyond maintains a strict policy of keeping all personally identifiable information confidential.

Achieve Beyond maintains all patient records in a secure electronic format. All hard copies are scanned into a secure network location and linked to the Achieve Beyond database. Electronic files are accessed by logging into the database. File access permissions are controlled by Windows Active Directory permissions. Database access requires a unique username and password and is not integrated with Windows authentication.

Any original documents that must be kept are labeled with the patient's and are locked in a secure cabinet. All other originals are scanned, and after they are shredded by a document security company.

Records containing Protected Health Information (PHI) in the possession of direct service providers or service coordinators must be secured appropriately. If records are kept in a provider's home, they must be stored in a locked cabinet. Files that are transported by service providers and service coordinators must be carried in fastened envelopes in locked attaché, brief cases or bags. Files should never be left unattended in vehicles. Copies that are no longer needed must be shredded.

Off Site Storage Policy

Records containing personally identifiable information in the possession of direct service providers or service coordinators must be secured appropriately. If records are kept in the provider's home, they must be stored in a locked cabinet. Files that are transported by service providers and service coordinators must be carried in fastened envelopes in locked attaché, brief cases or bags. Copies that are no longer needed must be shredded.

Achieve Beyond securely stores non-active children's files at a secure offsite storage facility. Once cases are closed, files are moved from locked cabinets at Achieve Beyond, sealed into boxes and transported directly to the storage facility.

Electronic Record Policy

Achieve Beyond maintains all child records in a secure electronic format. All hard copies are scanned into a secure network location and linked to the Achieve Beyond database. Electronic files are accessed by logging into the database. File access permissions are controlled by Windows Active Directory permissions. Database access requires a unique username and password and is not integrated with Windows authentication.

All children's records at Achieve Beyond are linked into a Database in order to facilitate staffing, track services, meet timelines, enter notes and bill. Staff must log in to gain access to system. The login is password protected.

© Copyright Achieve Beyond Pediatric Therapy & Autism Services 2018

Viewing and editing information is governed by need. Modifying permissions to view or edit information can only be granted by the Compliance Officer, Program Manager or IT Director.

Staff is not permitted to burn CDs, discs or DVDs of any child's file/record. If a request for such has been made by a parent or governing municipality, the IT Director will execute the request, perform the task and the item will be kept in a locked, secured cabinet until collected.

E-mail Security Policy

Each employee of the agency has an email account that is password protected and can only be accessed by that individual. Each user has a username. Users can change their passwords as needed. The passwords are saved in an encrypted format by Windows Active Directory.

A strict password policy is enforced for all email accounts. All passwords expire every 180 days. Also, all passwords must meet the following complexity requirements:

- Must be at least 8 characters in length
- Must contain at least 3 of the following 4 character groups: English uppercase characters (A through Z); English lowercase characters (a through z); Numerals (0 through 9); Non-alphabetic characters (such as !, $, #, %)
- Has not been used in the previous 24 passwords
- Must not have been changed in the last 2 days
- Does not contain your account or full name

Achieve Beyond maintains confidentiality in email by using a SSL(Secure Socket Layer) certificate issued by Go Daddy Secure Certification Authority. The SSL ensures that all communication between user and server takes place over an encrypted medium, wired or wireless. This way no external entity can maliciously gain access to sensitive information.

Confidentiality on the Achieve Beyond internal network is ensured by using security measures including a Microsoft Windows password, group policy and permissions and user-level security through Windows Active Directory. The servers, as well as clients, are regularly updated with the latest Microsoft updates to ensure security and confidentiality. All servers and clients are protected by a centralized enterprise Antivirus and Antispyware client. External users cannot access these files due to a firewall present between the internal Achieve Beyond network and the internet. The firewall has ports opened for Email and HTTP over SSL. All email exchange is performed through servers that are on site which is secured in a locked data center. Only on-staff IT Administrators have access to the data center.

Staff is not to send sensitive information to providers' personal email addresses. We have mandated usage of either their achievebeyondusa.com or Therapistemail.com or bilingualsinc.com email account as these email accounts are secure, all email communication is encrypted, and these email servers use the latest Microsoft Secure Email technologies.

In instances when employees work from home, they must use a secure VPN connection to our server that is authenticated by our firewall and then by Microsoft Windows servers hosted in the Achieve Beyond network. Employees can remotely login to our Database and email through

© Copyright Achieve Beyond Pediatric Therapy & Autism Services 2018

VPN which is secured using SSL technology. All employees must provide a private username and password for authentication. An alternative to VPN for email is Outlook Web Access (OWA). OWA also uses SSL technology and requires all employees to login for authentication. The SSL technology ensures the encryption using RSA algorithm. All remote connection servers, computers and the OWA front-end server are behind a CISCO ASA 5512 Firewall which accepts incoming connections on few selected ports.

Email transmissions via external email accounts will not include any personal "identifying" information regarding a child. The child's name or any personal identifying information will not be noted in any instance.

Emails will be sent and received by all staff members-administrative, service providers, evaluators, Service Coordinators, etc., on our encrypted, firewalled and secure SERVERS.

No email communication will take place outside our SERVERS. This SSL certificate will:

- Ensure the identity of the remote computer
- Prove the identity of the remote user to the computer
- Issuer of the certificate is: Go Daddy Secure Certification Authority
- RSA Key is 2048 bit encryption
- SHA-2 Algorithm

The usage of SSL guarantees authentication of our end users as well as confidentiality of our information.

Policy on the Use of E-Mail and Text Messaging to Communicate Patients' Protected Health Information

Achieve Beyond must maintain the confidentiality its patients' Protected Health Information or "PHI". PHI is information, transmitted or maintained in any form or medium, that relates to the:

- Past, present or future physical or mental health or condition of an individual provision of health care to an individual
- Past, present or future payment for the provision of health care to an individual;
- Identifies the individual in any way, including by name, social security number, finger print, or full face photographic images; and
- Has been created or received by a Covered Entity such as Achieve Beyond

Given that both e-mail and text messaging are dominant forms of communication, extra precaution must be taken when communicating PHI.

General E-mail Precautions

© Copyright Achieve Beyond Pediatric Therapy & Autism Services 2018

Achieve Beyond employees and contractors may only transmit PHI between Achieve Beyond e-mail addresses, as the company controls all security on the "achievebeyondusa.com" domain.

PHI is never to be transmitted to and from an outside e-mail address. Individuals should never communicate any information regarding a patient's treatment or payment/billing information to or from an outside e-mail address. Nor should an individual communicate a patient's name, social security number, date of birth or images and/or videos of the patient to or from an outside e-mail address.

Exceptions to E-mailing PHI to and from Outside E-mail Addresses

Employees and contractors may e-mail PHI to a parent/guardian of a patient if the parent/guardian gives written consent to e-mail PHI. All employees and contractors should verify that the respective parent/guardian has given written consent to e-mail with the appropriate Program Manager. Direct Service Providers should never directly accept written consent to e-mail from a parent/guardian without first consulting with the appropriate Program Manager.

Individuals may e-mail a password protected attachment (PDF, MS Word, MS Excel, etc) containing PHI to or from an outside e-mail address. PHI should only be contained in the password protected attachment and not in the body of the actual e-mail. The password to the attachment should be provided to the recipient via phone or a follow up e-mail. The password should never be contained in the body of the e-mail carrying the actual attachment.

Text Messaging

PHI should never be transmitted via text message. Information regarding treatment, the patient's name, Social Security number, date of birth or images and/or videos should never be communicated via text message. A Direct Service Provider may confirm treatment times or locations, without using patient name, via text.

Employees and contractors may communicate PHI via text to a parent/guardian of a patient if the parent/guardian gives written consent to text PHI. All employees and contractors should verify that the respective parent/guardian has given written consent to communicate PHI via text with the appropriate Program Manager. Direct Service Providers should never directly accept written consent to text from a parent/guardian without first consulting with the appropriate Program Manager.

© Copyright Achieve Beyond Pediatric Therapy & Autism Services 2018

Fax Confidentiality Policy

It is the policy of Achieve Beyond to protect the confidentiality and integrity of children, employee and business information when using fax machines to transmit or receive that information as required by law.

The following types of medical information are given special protection by federal and/or state law, and it therefore is Achieve Beyond's policy that such information may NOT be faxed or photocopied for use outside Achieve Beyond without specific written parent authorization unless otherwise authorized or required by law, a court order or judicial subpoena:

- HIV status
- Sexual or physical abuse
- Treatment for mental illness
- Child's parentage

Program Director is responsible for locating fax machines in secure areas that have limited access. The first page of each fax transmission should be the Achieve Beyond fax cover page and should include the following information: sender's name, sender's voice number, sender's fax number, recipient's name, recipient's voice number, recipient's fax number, transmission date and time, and number of pages including the cover sheet and the Achieve Beyond standard confidentiality statement:

"CONFIDENTIALITY NOTICE: This message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information or other use be protected by law. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please inform sender immediately and destroy all copies of the original message."

The sender must limit the information transmitted to the minimum necessary to meet the requestor's needs. For confidential documents, the cover page must be marked "confidential" before they are transmitted. The sender must ensure the fax is sent to the correct destination. The sender must verify the fax number before sending the fax and verify the recipient's authority to receive confidential information. The sender must receive a fax confirmation once the fax has been sent. Also, the sender must report any misdirected fax to the Program Director immediately.

Each department is responsible for ensuring that incoming faxes are properly handled. A fax should not be left sitting on or near the machine, but rather should be distributed to the proper recipient expeditiously while protecting confidentiality during distribution, such as by sealing the fax in an envelope. All faxes are received into a fax server and distributed via email to the proper recipient. Any confidential information faxed to Achieve Beyond in error will be destroyed, and the sender notified.

© Copyright Achieve Beyond Pediatric Therapy & Autism Services 2018

Policy on Access to Records

All children's records at Achieve Beyond are linked into a Database in order to facilitate staffing, track services, meet evaluation timelines, enter service coordination notes, and bill. Staff must log in to gain access to system. The login is password protected.

Each time a user logs-in to the Database to access a child record, the Database automatically calculates the date and time of access, the name and ID number of the child, and the name of the user. The purpose of the access can be identified and determined based on the user name. This information is stored in the Database, and may be obtained via an access log report, if and when needed. A separate access log sheet is used for those who do not routinely access the file. A record is kept of all individuals, other than authorized individuals, who access a child's record which includes the name of the party accessing the record, the date of access, and the purpose for which the record was accessed. Only authorized administrative staff and service providers who are currently working with the child will have access to the child's records.

Viewing and editing information is governed by need. Service provider personal information is available only to the Human Resources and Compliance Departments. Data Management Supervisor, Early Intervention Program Director, the Assistant Director, Executive Director, Operations Manager, Compliance Officer and Quality Assurance personnel can view all information.

Clinical Student Interns do not have access to the files. If necessary, the practicum supervisor (an Achieve Beyond employee) may share relevant information with the interns. Clinical Interns may not use any child's information that violates the confidentiality rights of the child. Any report written by staff or interns is the property of Achieve Beyond and is to be maintained as such in the child's file.

Staff is not permitted to burn CDs, discs or DVDs of any child's file/record. If a request for such has been made by a parent or governing municipality or payor, the IT Director will execute the request, perform the task and the item will be kept in a locked, secured cabinet until collected.

Parental Access to Records

It is the policy of Achieve Beyond to adhere to state and federal laws and regulations regarding access to children's educational records.

Parents/legal guardians have access to all documents and reports contained in their child's record. At the beginning of service by Achieve Beyond, parents/guardians are informed of the right to access their child's records, an understandable explanation of the records and the right to amend their child's records.

Upon verbal or written request to the Program Manager or Compliance Officer, parents will receive copies of all reports found in their child's file. Whenever requested, Achieve Beyond

© Copyright Achieve Beyond Pediatric Therapy & Autism Services 2018

staff will arrange to discuss the content of the reports. The completed request form or letter from the parent will be filed. Copies will be provided at no charge to families.

The Compliance Officer will ensure that requests from parents/legal guardians for copies of the child's record will be sent no later than 10 working days from the receipt of the request, or within 5 days if the request is made as a part of mediation or an impartial hearing. The parent/legal guardian has the right to have a representative view the child's record on their behalf.

If the record contains information on more than one child, the parent/guardian is only allowed to view information that pertains to their child. The Compliance Officer will ensure that information regarding other children is "blacked out" before it is turned over.

Amending Child Records

The parent/guardian has the right to request an amendment to their child's record when the parent believes the information contained in the record is inaccurate, misleading, or violates the privacy or any other rights of their child. At the beginning of service by Achieve Beyond, parents/guardians are informed of the right to access their child's records, an understandable explanation of the records and the right to amend their child's records.

Achieve Beyond will respond to the parent's request within 10 business days. If the Achieve Beyond decides not to amend the record as requested, the Program Manager or Compliance Officer informs the parent/guardian of the decision.

If the information in the record is found to be inaccurate, misleading or to violate the privacy of the child/family, the provider will amend the information and will inform the Program Manager or Compliance Officer. The Program Manager or Compliance Officer will notify the parent/guardian of the amendment.

Achieve Beyond assumes all parents/guardians have authority to review their children's records unless informed that a parent/guardian is not allowed access under applicable state law governing matters such as guardianship, divorce or separation.

Record Requests for Unauthorized Individuals

Achieve Beyond will not release child records to unauthorized individuals, such as attorneys, without written consent from the child's parent/guardian.

Record requests from attorneys with authorization signed by the parent/guardian will be charged at the rate of $0.10 per page for the first set and $0.25 per page for the subsequent sets of records, as long the fee charged does not prevent the parent from inspecting and reviewing of the record.

© Copyright Achieve Beyond Pediatric Therapy & Autism Services 2018

Protection of Sensitive Information

It is the policy of Achieve Beyond to maintain files in accordance with state and federal laws and regulations. These statutes require that children's files be kept secured and confidential. Information which is not directly relevant to his/her clinical or educational needs will not be maintained in the child's record. Personal notes must not be placed in the child's record and cannot be used in making decisions for referral, evaluations or services.

All staff writing reports for the files must limit the contents of the reports to those topics relevant to a child's developmental, therapeutic and educational needs.

Upon receipt of reports from outside sources, the Achieve Beyond Program Director and/or designee will ascertain the relevance of the contents to the specific child.

When a report is stamped "privileged and confidential" a decision must be made as to the relevance to the current clinical and educational needs of the child. This decision should be made in view of the fact that Achieve Beyond is required to release this document to parents of children. If relevant, it is filed. If the Program Director or designee judges that the report contains items not relevant to the child's developmental and educational needs, it will be returned to the source for revision.

Sensitive information such as sexual or physical abuse, HIV status, treatment for mental illness, domestic violence and the child's parentage, etc., should not be included in reports or case notes. The source must be reminded that parents have the right to all reports, notes, paperwork, etc., in its entirety, and that the sharing of this type of information can be compromising and demeaning to the family. Where appropriate, the child may need to be re-evaluated and a new report written.

When information about a child/family is contained in records that include information about multiple children, only information pertaining to that child/family can be released. Personally identifiable information about others will be protected.

All Achieve Beyond employees and service providers will adhere to, implement, and maintain the policies and procedures to assure the protection of confidential personally identifiable information pertaining to each child. All employees and contractors must sign off on a Confidentiality Policy.

Any breach of confidentiality (such as loss or theft of records) must be reported to the Compliance Officer no later than one (1) week of post discovery.

HIV-Related Information

Achieve Beyond maintains the confidentiality of individuals diagnosed as having AIDS or HIV-related illness, HIV infection or laboratory tests for HIV-related illness. Achieve Beyond will

© Copyright Achieve Beyond Pediatric Therapy & Autism Services 2018

only disclose HIV-related information with prior written consent of the parent or guardian. Any disclosure of HIV-related information shall be accompanied by the following statement:

"This information has been disclosed to you from confidential records, which are protected by State law. State law prohibits you from making any further disclosure of this information with specific written consent of the person to whom it pertains, or as otherwise permitted by law. Any unauthorized further disclosure in violation of State law may result in a fine or jail sentence or both. A general authorization for the release of medical or other information is NOT sufficient authorization for further disclosure."

Storing Client Information on Personal Computers, Tablets, Mobile Phones, Disks, CDs, USB/Flash Drives and External Hard Drives

Protecting the personally identifiable information of our clients is paramount to the Compliance & IT Security functions of Achieve Beyond. Employees and Independent Contractors using their own personal Computers, Tablets, Mobile Phones, Disks, CDs, USB/Flash Drives and External Hard Drives to store patient information must take extra precaution.

Personal Computers/Laptops

In order to create the most secure environment for information stored on your personal computer/laptop, Achieve recommends the use of a strong password. Passwords should be at least six characters with one capital letter and one number. Computers should be locked or turned off when not in use.

All office staff who have access to Achieve Beyond's network via VPN should not work on or store client information outside the VPN environment.

Tablets and Mobile Phones

All personal tablets and mobile phones that may be used to communicate or store patient data should be password protected. Phones should be set to lock after a minimum of 5 minutes of inactivity. If you upload your Achieve Beyond e-mail address to your personal tablet or phone, you will be automatically forced to use these password guidelines.

Disks, CDs, USB/Flash Drives and External Hard Drives

Achieve Beyond recommends encrypting all documents files containing patient data on Disks, CDs, USB/Flash Drives and External Hard Drives with a password. Passwords should be at least six characters with one capital letter and one number. Disks, CDs, USB/Flash Drives and External Hard Drives should be kept in a locked bag or case when not in use.

© Copyright Achieve Beyond Pediatric Therapy & Autism Services 2018

Transportation and Storage of Personal Devices

Any personal electronic device that may contain client information should be transported in a locked bag or case and only removed when in actual use. Personal devices should never be left unattended in vehicles..

Lost or Stolen Personal Devices

IF A PERSONAL DEVICE THAT CONTAINS CLIENT INFORMATION IS LOST OR STOLEN, PLEASE CONTACT THE RESPECTIVE PROGRAM MANAGER, THE COMPLIANCE OFFICER OR THE IT DEPARTMENT IMMEDIATELY.
If your lost or stolen tablet or mobile phone has your Achieve Beyond e-mail uploaded, the IT department will remotely wipe the device clean for your protection.

Video Taping/Filming of Patients

Achieve Beyond employees and contracts are NOT to video tape or film patients without written consent from the respective parent/guardian. If an Achieve Beyond employee or contractor wishes to obtain written consent from a parent/guardian, they are to contact and receive approval from their respective Program Manager PRIOR to requesting consent to videotape/film from the parent/guardian.

© Copyright Achieve Beyond Pediatric Therapy & Autism Services 2018