HANDLING OF PROTECTED HEALTH INFORMATION

**Policy**

1. Medical record data of each person served along with the individual’s medical file data and related financial, demographic, and lifestyle information is sensitive and confidential.
2. Siyan Clinical shall monitor and keep the privacy of current and former persons served, (be they deceased or living). Medical and other sensitive material that has been transmitted to, within, or sent from Siyan Clinical shall be protected in accordance with our program’s Code of Conduct
	1. All staff members, whether clinical or administrative, shall maintain the integrity of confidentiality of the individual’s information and medical records.
	2. Employees shall investigate and report any threats to the breaches of confidentiality to their immediate supervisor.
3. Siyan Clinical shall ensure that all staff and/or contractors have the necessary protected health information to provide high quality services, while protecting the confidentiality of the individuals served.
4. Siyan Clinical shall not use or provide private medical information for non-healthcare uses, such as employment, credit evaluation, direct marketing, or any other reasons outside of direct service provision.
5. Siyan Clinical staff shall but forth their best efforts to ensure the accuracy, timeliness, and completeness of data that is documented within the individual’s medical record.
6. Siyan Clinical staff shall complete and authenticate medical records in accordance with the law, medical ethics, and accreditation standards.
7. Siyan Clinical staff recognize that the persons served have rights to maintaining the integrity of their health information.
8. Siyan Clinical shall maintain medical records for the retention periods require by law and professional standards, whichever is longest.
9. In the interest of effective care coordination, Siyan Clinical shall obtain a signed authorization to release information for the individual’s primary care physician, mental health provider, and/or another treating physician.
10. Breaches and security incidents involving the unauthorized access, use, modification, disclosure, or destruction of protected health information are types of critical incidents.
	1. It is each employee’s responsibility to know what a breach is and how to report it to management.
	2. Suspected breaches should always be reported to management who shall make a notation about this suspected or confirmed breach within the participant’s medical record and to DHCS in writing.

**Procedure**

As part of their orientation, employees shall receive HIPAA training and training on Siyan Clinical’s policy on maintaining the confidentiality of persons. Trainings will occur during new hire orientation and annually thereafter.

Siyan Clinical’s staff shall collect and use individual medical information only for the purposes of providing services and to support the payment, delivery, integrity, and quality of the services.

Siyan Clinical staff shall collect and use the individual’s confidential information:

* To provide proper diagnosis and treatment.
* With the individual’s knowledge and consent.
* To receive reimbursement for delivery of treatment services.
* For research designed to maintain and improve service quality.
* As a basis for reporting protected health information according to state and federal guidelines.

**Additional Medical Record Guidelines**

1. Siyan Clinical staff shall not alter or destroy an entry in any medical records. Instead, staff shall identify an entry as an error by adding an addendum to the medical record correcting the documented error. The original erroneous entry shall remain intact and readable.
2. All medical records shall be treated as confidential in accordance with the professional ethics, standards, and other legal requirements both federal and state.
3. Staff shall not share medical records or the data within the record unless the person served, (or the individual’s legal representative), has consented to the release in writing or the release is authorized by law, such as Tarasoff, child abuse reporting, dependent adult, and elder abuse reporting, or if the person served is a danger to themselves or to others.
4. When Siyan Clinical staff releases data from an individual’s medical record, the program will take appropriate steps to ensure that unauthorized redisclosures by specifying that the recipient may not further disclose the information without the consent of the person served or as authorized by law.
5. All releases of information forms, fax cover sheets, or email signatures footers shall also include a statement that the information included may contain confidential information that shall not further be released and to notify Siyan Clinical if information was received by an unintended recipient.
6. Siyan Clinical staff shall not disclose financial or other information except as necessary for billing or other authorized purposes.
7. Siyan Clinical shall not sell, share, or use the individual’s medical information for any reason or purpose that is not necessary to provide health care services.
8. Siyan Clinical staff shall be trained regarding sensitive medical information such as HIV/AID status, mental health information, developmental disability, therapy notes, alcohol and drug abuse information, and other information about communicable diseases.
	1. Siyan Clinical staff shall handle this information with confidentiality as required by law, professional ethics, and accreditation requirements.
9. Siyan Clinical staff shall recognize that the person served has the right to access this information that is kept within the medical record.
	1. Siyan Clinical staff shall allow and permit the person served to access their medical record, except when access to this file would be detrimental to the person served under the therapeutic exception to access.
	2. In these cases, Siyan Clinical staff shall provide the authorized representative access to these records in accordance with law, professional ethics, and regulatory requirements.
	3. If there is ever a question about such a case, the Medical Director shall be consulted for the final determination of how and whether the information should be released.
	4. If the person served reviews the medical record and recognizes errors within this record, Siyan Clinical staff shall provide an opportunity for the person served to correct the inaccuracies within the record in accordance with the law and ethical standards.
	5. If a correction is made, procedures regarding keeping the error intact, yet making the corrections obvious enough so an authorized reviewer may be able to recognize the error(s) and the correction(s).
10. Siyan Clinical staff shall adhere to this policy and procedure. Violation of this policy is grounds for disciplinary action for Siyan Care staff up to, and including, termination of employment.
	1. Progressive disciplinary action may include criminal and/or professional sanctions in accordance with respective legal and professional agencies and accreditation bodies.

**Suspected Breach of Confidentiality, Procedure**

1. A breach is the acquisition, access, modification, destruction, or use or disclosure or protected health information (PHI) by staff in a manner that is not permitted by Federal and State laws and regulatory requirements.
	1. All staff members shall receive HIPAA Compliance training to ensure continued protection of all clients’ Protected Health Information.
2. The staff who became aware of the potential breach must complete a Privacy Incident Report form and submit it to their supervisor. The supervisor shall then contact their DHCS privacy representative (incidents@dhcs.ca.gov) to report the breach and arrange to send the incident form detailing information regarding the security incident or breach along with any additional information regarding the PHI which has the potential to be, or has already been, accessed or acquired by an unauthorized person.
3. A breach shall be treated as discovered as of the first day that the breach is known or should have been known to any person exercising reasonable diligence.
	1. Here “any person” is identified as the person who committed the suspected breach, or any other person who is an employee, officer, contractor, or other agent of Siyan Clinical.
4. If a significant breach or security incident happens after hours, (to include weekend or holidays), that poses harm to clients, Siyan Clinical management shall immediately address the incident by completing the Incident Report and emailing it to incidents@dhcs.ca.gov.
5. For all breaches, Siyan Clinical management staff shall submit a DHCS “Privacy Incident Report” or, (Special Incident Report/Unusual Occurrence Report), within 24. Any breach of Social Security Administration information) to the DHCS Information Protection Unit (IPU) at the Office of HIPAA Compliance (OHC) is also included in this procedure.
	1. The initial “Privacy Incident Report” will contain all required information to the extent known at that time of filing. Siyan Clinical will follow further instructions received from the IPU. Management shall notify DHCS by calling the Information Protection Unit (916- 445-4646, 866-866-0602) and emailing notification to: privacyofficer@dhcs.ca.gov Updated forms will be submitted to the DHCS as more information becomes available.
	2. This information shall also be logged internally to be discussed at the next Quality Improvement Committee meeting to ensure appropriate performance improvement initiatives are implemented.
	3. However, if any changes can be made immediately to ensure that the breach will not be repeated, management is responsible for making those changes immediately and informing the Medical Director to ensure that the changes in policy and/or procedure fall within compliance guidelines of governing authorities, mainly, DHCS and HIPAA.
	4. If a change in policy and/or procedure takes place, an emergency meeting shall be held to inform staff about the changes and staff shall sign an acknowledgement of receipt and understanding regarding the new policy and procedure.
6. A managerial review is required for all incidents.
	1. The review shall include a root cause analysis and identification of performance improvement measures to prevent future occurrences.
	2. Management, including the Medical Director, shall monitor the improvements or otherwise address issues identified in the Critical Incident Report.
	3. No copies of the original report are to be made or retained by Siyan Clinical staff and only a copy is allowable to be maintained by the Quality Improvement officer.

**Certified Community Behavioral Health Center (CCBHC) Services and Consent to Participate**

As a CCBHC, we are required by SAMHSA to collect information on patients/clients who receive services at our CCBHC. The information collected is only done so to help us show that our CCBHC is effective at serving our patients/clients. Any client who accepts services at the CCBHC will be asked to provide confidential information, which we will not share directly with SAMHSA or anyone else in any way that identifies the client. Client participation will be strictly confidential.

Because we are only reporting on combined data from all patients/clients collectively, it is highly unlikely that any information that we produce will in any way identify children or adults participating in the program. As with all medical information and medical records, we are committed to protecting clients’ privacy. Furthermore, information gathered during client participation is stored in secure locations that only selected individuals are permitted to access.

Additionally, Siyan developed CCBHC-specific consent forms as listed below:

* Consent to Participate in Data Collection
* General Information and Consent for Treatment
* Release of Information
* Patient Responsibility and Financial Agreement Template
* Medication Refill Policy
* HIPPA and Patient Confidentiality

These forms will be reviewed with each CCBHC client and signed prior to their final enrollment in the CCBHC program.