HIPAA Manual

Victor Treatment Centers
1360 East Lassen Avenue
Chico, CA 95973

March 2017

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) MANUAL

Introduction

Victor is a unique partnership of two organizations – Victor Treatment Centers and Victor Community Support Services – dedicated to serving the most troubled children throughout California. One of Victor's core beliefs is that children and families benefit most from supportive services when such services are provided in the communities where they live and attend school. Wherever a family's need takes us, the protection of consumer privacy is of utmost importance to Victor. This HIPAA Compliance Manual contains Victor Treatment Center's policies, procedures, and standards of conduct designed to ensure its compliance with applicable federal and state laws, and regulations governing the privacy of the health records of the children it serves.

Mission Statement

Our mission is to be a catalyst for sustained improvement in the lives of those we touch. At all times, Victor endeavors to maintain the highest degree of integrity in its interactions with the children and families it serves. Our mission statement, therefore, drives our commitment to maintain compliance with all laws, rules, and regulations affecting the delivery of behavioral health care and the handling of private consumer information.

Designation of Privacy and Security Officer

Victor Treatment Centers is comprised of residential treatment facilities and non-public schools. Approximately 400 professional and paraprofessional staff deliver the services provided at these programs. Due to the size of Victor, there is a need to create a standardized and uniform approach to the handling of the Protected Health Information (PHI) of our consumers. To meet this need, one individual shall fulfill the role of the Agency's Privacy Officer, and one individual shall fulfill the role of the Agency's Security Officer.

The responsibilities of these roles are as follows:

Privacy Officer

The Director of Compliance or designee serves as the Agency Privacy Officer and is responsible for the development, implementation, and maintenance of the Agency's privacy and compliance-related activities. The Privacy Officer ensures that Agency-wide practices, policies, and procedures related to privacy issues are compliant with federal, state, and local regulations. Examples of the Privacy Officer's duties include, but are not limited to the following:

- Oversee and monitor implementation of the Privacy components of the HIPAA Compliance Plan.
- Establish and serve as facilitator of the Compliance Workgroup, which is charged with monitoring regulatory requirements, developing an Agency-wide privacy program and implementing appropriate strategies to promote HIPAA compliance.
- Develop and implement a training program focusing on the privacy components of the HIPAA Compliance Plan, and ensure that training materials are appropriate for each class of Victor employee – management, administrative, direct care, and clinical.
- Ensure that independent contractors who provide services to Victor consumers are aware of, and agree to follow, the privacy practices set forth in the HIPAA Compliance Plan.
- Coordinate Victor's privacy compliance efforts within the Agency, and establish methods to reduce the Agency's vulnerability to privacy policy abuse.
- Conduct periodic audits to ensure that the Privacy Policies and Procedures are being implemented across the Agency.
- Periodically revise the HIPAA Compliance Manual and associated documents, including the Notice of Privacy Practices, Release of Information, Requests to Access/Amend Records, Requests to Restrict Access, and Denial of Access or Amendment, in light of changes in the law.
- Develop mechanisms to receive and investigate reports of privacy breaches and monitor subsequent corrective action.
- Collect information regarding privacy breaches Agency-wide, and prepare and submit annual reports to Health and Human Services (HHS).

- Coordinate with appropriate Legal Counsel and Human Resources personnel to develop and monitor appropriate sanctions policies for failure to comply with the Agency's privacy program.
- Prepare and present regular reports to the Board of Directors, and Agency as a whole, on privacy practice compliance.

Security Officer

The Security Officer serves under the direction of the Director of Administrative Services and is responsible for the ongoing management of information security policies, procedures, and technical systems in order to maintain the confidentiality, integrity, and availability of all of Victor's healthcare information systems. Examples of the Security Officer's duties include, but are not limited to the following:

- Oversee and implement Security components of the HIPAA Compliance Plan.
- Develop and implement a training program focusing on the security components of the HIPAA Compliance Plan, and ensure that training materials are appropriate for each class of Victor employee – management, administrative, and clinical.
- Ensure that independent contractors who furnish medical services to the Agency are aware of the security requirements of the HIPAA Compliance Plan.
- Coordinate security compliance efforts within the Agency, and conduct periodic audits to ensure that information systems are adequately protected and meet HIPAA certification requirements.
- Ensure that the access control, disaster recovery, business continuity, incident response, and risk management needs of the Agency are properly addressed.
- Work with vendors, outside consultants, and other third parties to improve information security within the organization.
- Lead an incident response team to contain, investigate, and prevent future computer security breaches and monitor subsequent correction actions.

Written Policies and Procedures

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) mandated significant changes to the healthcare industry; it applies to health care providers and

employer group health plans. HIPAA is a complex statute that affects Victor in several ways, including its operations, policies, Information Technology (IT) systems, contractual relationships and relationships with community partners. In general, HIPAA was designed to protect individual privacy by establishing standards for the exchange of health information, establishing security standards, and establishing privacy standards for the use and disclosure of health information.

Significant changes to HIPAA came in 2009, when Congress amended the statute through the enactment of the Health Information Technology for Economic and Clinical Health Act (HITECH). HITECH promotes the use of Electronic Health Records (EHRs) across the healthcare industry. Because the use of electronic records creates new and additional risks for providers, Congress recognized a need to strengthen the privacy and security of protected health information to reduce risks associated with electronic record-keeping systems. The changes made by way of HITECH are not solely aimed at providers implementing EHRs. Many changes, such as enforcement provisions, rules for Business Associates, and notification of privacy or security breaches apply to all healthcare providers, whether or not they are using an EHR.

The policies and procedures identified in Appendix A and B of this Manual address the three major requirements Victor must meet to fully comply with HIPAA and HITECH: protection for the privacy of Protected Health Information (PHI), protection for the security of PHI, and standardization of electronic data transactions. At a minimum, each program across Victor is expected to implement the provisions of the written policies and procedures identified below.

Policies for Consumer Privacy

- Consumer Privacy Rights
- Designation of a Local HIPAA Representative
- Mandatory Breach Notification
- Minimum Necessary Uses, Disclosures, and Requests
- Notice of Privacy Practices
- Release of Information or Authorization to Release Information

- Release of Information to a Personal Representatives or Person Involved in a Consumer's Care
- Response to Subpoenas and Court Orders
- Uses and Disclosures of PHI for Marketing and Fundraising
- Workforce Agreement to Adhere to Privacy and Security Policies

Policies for Security of Consumer PHI

- Access Authorization, Establishment and Modification
- Acquisition and Decommissioning Leased/Owned Imaging Equipment
- Automatic Log-Off Policy
- Data Backup and Storage Policy
- Email Acceptable Use Policy
- Encryption and Decryption Policy
- Facility Security Policy
- Facsimile Transmission of PHI
- Hardware and Media Accountability Policy
- HIPAA Security Training Policy
- Information Systems Activity Review Policy
- Log-In Monitoring Policy
- Password Management Policy
- Security Incident Policy
- Security Reminders Policy
- Virus and Malware Protection Policy
- Workstation Use Policy

Internal Monitoring and Auditing

Every Victor employee is required to be familiar with the HIPAA Compliance Plan, and to fully cooperate with the Privacy and Security Officers as requested. The local HIPAA representative and the Agency Privacy and Security Officers shall conduct periodic audits of critical operations subject to HIPAA laws and regulations at each of the Victor programs. These audits shall focus on general compliance with established privacy and security policies and procedures. The Agency Privacy and Security Officers shall

generate reports to summarize audit results, which shall be shared with the Compliance Workgroup, Executive Leadership, and the COO/CEO.

These periodic audits shall be conducted at least annually, or as often as indicated at each of the programs. Based on the results of these audits, the Privacy and Security Officers shall make adjustments to HIPAA training and policies. Where corrective action at the program level is required, the Privacy and/or Security Officers shall thoroughly monitor until compliance is accomplished. If, based on an audit, an employee is found to have acted in a manner that is in direct violation of the established policies and procedures, the Privacy and/or Security Officer, in conjunction with Human Resources Director, shall take appropriate remedial action.

Training and Education

All Victor employees shall receive HIPAA training at hire through New Hire Orientation. Each employee shall be required annually to sign the Workforce Agreement to Adhere to Privacy and Security Policies (Attachment A - HF 05). Thereafter, every Victor employee shall receive annual training that shall equip them with knowledge on how to perform their respective jobs in compliance with Agency HIPAA policies and procedures and any applicable state or federal regulations. The overarching goal of annual trainings is to impress upon all employees that HIPAA compliance is a condition of continued employment. All employees shall sign an annual HIPAA acknowledgment form (Attachment A - PF 88) and an Electronic Signature Agreement form (Attachment A - PF 365a).

In addition, the HIPAA representative at the local programs shall provide HIPAA awareness updates as needed. These updates may address a variety of HIPAA issues that are present in the daily work environment, and shall be geared towards early detection and resolution of HIPAA related risks.

Open Lines of Communication

Victor employees who wish to report HIPAA compliance issues can do so with his/her immediate supervisor, program HIPAA representative, Executive Director, the Agency

Privacy or Security Officer, or members of the Compliance Workgroup. If they wish, they can make such reports in person, by phone, through written correspondence, or anonymously at the Agency's toll free Compliance number (888-881-1802) . When reporting HIPAA compliance issues, employees shall include: 1) the date and nature of the incident, 2) date of report, 3) program involved, and 4) person involved in the suspected compliance incident.

All reports of actual or suspected non-compliance are given to the Privacy and Security Officers regardless of the manner in which the report was made. The Privacy and Security Officers shall review the reports to determine the appropriate response, including notification of any individual affected by a breach of privacy or security of PHI. At the conclusion of each fiscal year, the Privacy Officer shall prepare a summary of all HIPAA compliance incidents, which shall be submitted to HHS, the CEO, and the Board of Directors.

Response to Detected Problems

When an issue of actual or suspected non-compliance with the HIPAA policies and procedures is identified, the program's HIPAA representative and Privacy Officer shall be notified. At this point, the two parties shall review the incident together and determine the appropriate response. The review of the incident shall focus on:

- An assessment of the breach or act of non-compliance.
- Risk assessment for harm to the individual(s) affected.
- The appropriate breach notification, if any.
- Mandated reporting, if any.

Each of these considerations shall be made timely, so that the notification provided to affected consumers shall be made in compliance with HIPAA and HITECH regulations. In addition, an action plan shall be developed at the affected site to avoid future incidents of non-compliance, clarify expectations of the workforce, and provide additional training where indicated.

Adherence to Disciplinary Standards

Victor makes disciplinary decisions on an individual basis, taking into consideration the nature of the employee conduct and its impact on Victor consumers. Personnel action may include, but is not limited to, additional training, reduced responsibility, reassignment, increased supervision, demotion/transfer, suspension, or termination. All employees have a responsibility to ensure that Victor's Privacy and Security policies are implemented, which includes a responsibility to report actual or suspected incidents of HIPAA non-compliance. The Agency adheres to federal and state laws which prohibit retaliation, and therefore, no employee shall be subject to retaliation or discipline for making good-faith reports of suspected non-compliance.

Attachment A

1) **Client Protected Health Information Privacy and Security Workforce Agreement – HP 05**

2) **HIPAA Training Documentation – PF 88**

3) **Electronic Signature Agreement – PF 365b**

CLIENT PROTECTED HEALTH INFORMATION PRIVACY AND SECURITY WORKFORCE AGREEMENT

The Agency is committed to maintaining the confidentiality and security of "client Protected Health Information" (PHI), as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Client protected health information refers to any individually identifiable health information or behavioral healthcare information transmitted or maintained in any form. All workforce of the Agency who view PHI in paper or electronic form, email, or through access to individual department workstations, networks, and databases must read and comply with Agency policies under the Privacy and Security Rule and HIPAA law.

Under HIPAA law, the Agency is required to have and apply appropriate sanctions against workforce members that fail to comply with Agency privacy policies and procedures for the protection of health information. Workforce members are defined as: employees, contractors, volunteers, interns, temporary employees, and others whose conduct, in performance of work for the organization, is under the direct control of the organization.

Retraining, corrective action plans, verbal warnings, written warnings, disciplinary suspensions without pay, and terminations are possible disciplinary actions for violating Agency privacy policies and procedures for PHI. Management considers the seriousness of the infraction in order to determine the level of discipline required. Notices of disciplinary action are placed in the employee's personnel file.

All employees, contractors, interns, temporary employees, and volunteers are required to sign a *PHI Privacy and Security Workforce Agreement* that states that they comprehend, honor, and adhere to policies and procedures for privacy and security of client protected health information under HIPAA law, as well as understand the consequences for non-compliance. A copy of the signed *PHI Privacy and Security Workforce Agreement* is retained in the personnel file.

WORKFORCE ACKNOWLEDGMENT OF RESPONSIBILITIES FOR THE PRIVACY AND SECURITY OF PHI

Minimum Necessary Use and Disclosure of Client Protected Health Information
It is the policy of the Agency that all routine and recurring uses and disclosures of PHI, except for uses or disclosures made for the purpose of treatment, or as required by law for HIPAA compliance, must be limited to the minimum amount of information needed to accomplish the purpose of the use or disclosure. It is also the policy of the Agency that non-routine uses and disclosures are handled pursuant to established criteria and that all requests for client protected health information (except as specified above) must be limited to the minimum amount of information needed to accomplish the purpose of the request.

Complaints

It is the policy of the Agency that all complaints relating to the protection of health information be investigated and resolved in a timely fashion. Complaints must be addressed to the Agency's Privacy Officer, who is duly authorized to investigate complaints and implement resolutions if the complaint stems from a valid area of non-compliance with the HIPAA Privacy and Security Rule.

Prohibited Activities-No Retaliation or Intimidation

It is the policy of the Agency that: No workforce member may engage in any intimidating or retaliatory acts against persons who file complaints or otherwise exercise their rights under HIPAA law. It is also the policy of the Agency that no workforce member may condition treatment, payment, enrollment, or eligibility for benefits on the provision of an authorization to disclose client protected health information except as expressly authorized under HIPAA law (see Personnel Policy and Employee Handbook).

Cooperation with Privacy Oversight Authorities

It is the policy of the Agency that "oversight agencies" such as the Office for Civil Rights of the Department of Health and Human Services be given full support and cooperation in their efforts to ensure the protection of health information within this organization. It is also the policy of the Agency that: all workforce members cooperate fully with all privacy compliance reviews and investigations.

Personnel Clearance

It is the policy of the Agency that all workforce members be cleared before access to client protected health information is allowed.

Authentication

It is the policy of the Agency that all information system users be authenticated before access to information processing resources is allowed. Specifically, each user must have his or her individual system account, and passwords must never be shared outside of Agency protocol.

Media Access Control

It is the policy of the Agency that reusable media, such as tapes, zip disks or diskettes, must be securely erased or otherwise destroyed, before being discarded to prevent unauthorized access to health information.

Physical Access Control

It is the policy of the Agency that areas in which client protected health information is stored be posted off limits to all but authorized personnel. It is also the policy of the Agency that such areas be locked when unattended.

Workstation Use Guidelines

It is the policy of the Agency that all workstations be positioned in such a manner as to avoid accidental, unauthorized exposure of client protected health information. It is also the policy of the Agency that displays be locked when unattended.

Secure Data Transmission

It is the policy of the Agency that data communications that contain client protected health information be encrypted if they traverse public networks such as the Internet. It is also the policy of the Agency that all data transmission methods incorporate data integrity and authentication controls.

☐ VTC ☐ VCSS (Check one)

As a member of the Agency workforce
I will:

Please read carefully. Signing your initials states that you understand and agree to the following:	**Initials**
1. *Respect the privacy and security rules governing the use and disclosure of any client protected health information that is accessible to me through, paper records, computer system or network, and only utilizes information necessary for performance of my job.*	
2. *Not exhibit or divulge the contents of any record or report containing client protected health information except to fulfill a work assignment and in accordance with* Agency *policies and procedures for the privacy and security of PHI.*	
3. *Prevent unauthorized use and disclosure of any client protected health information in files maintained, stored, or accessible in my computer workstations or work areas.*	
4. *Respect the confidentiality of any reports printed from any information system containing client protected health information, and handle, store and dispose of these reports appropriately.*	
5. *Not remove any record (or copy) or report containing client protected health information from the office where it is kept except in the performance of my duties.*	
6. *Not divulge any information that identifies a client to other persons except in the performance of my duties.*	

7. *Understand that the information accessed through* Agency *Information Systems contains sensitive and confidential client care, business, and financial information that should only be disclosed to those authorized to receive it.*	
8. *Not release my authentication code or device to anyone else, or allow anyone else to access or alter client protected health information under my identity*.	
9. *Not utilize anyone else's authentication code or device in order to access* Agency *Information Systems.*	
10. *Observe the procedures established to manage the use, and protect the integrity of the Agency Information Systems.*	
11. *Understand that all access to* the Agency *Information Systems will be monitored.*	
12. *Report any violation of this agreement*.	
13. *Understand that my obligations under this Agreement will continue after termination of my employment.*	

I understand that my access to client protected health information maintained by the Agency is a privilege and not a right afforded to me. By signing this agreement, I agree to protect the privacy and security of this information and maintain all client protected health information in a manner consistent with the requirements outlined under federal privacy and security regulations of HIPAA law. Any breech of the terms outlined in this agreement will subject me to penalties, including disciplinary action, under policies of the Agency as well as any applicable state law. By signing this agreement, I agree that I have read, understand, and will comply with all the conditions outlined in this agreement.

Signature and Title

Date

HIPAA TRAINING DOCUMENTATION

☐ Initial Training ☐ Annual Re-Certification

I, _____ clearly understand the Agency's procedures, effective this date, related to safeguarding the Protected Health Information (PHI) of every individual. I have been made aware of the laws and guidelines that I must follow in order to meet this standard. I attest to the following statements and conditions.

I have completed the HIPAA training presentation that is required.

I have read, understand, accept, and have signed the required Agency Staff Privacy and Security Agreement statement documentation HF 05 (at New Hire).

I agree to follow the prescribed Agency guideline(s) that meet or may exceed the legally mandated privacy and security requirements.

I certify that I have read, understand, accept, and have completed the above steps and statements as conditions of my employment.

_____ _____
(Signature) (Date)

_____
(Print Name)

_____ _____
(Instructor/Witness) (Date)

(Personnel Form 04-88 – March 22, 2004) (Revised Date—August 31, 2011)

PF 11-88

Electronic Signature Agreement

This Agreement governs the rights, duties, and responsibilities of _____ Victor Treatment Centers, Inc. employee in the use of an electronic signature. I, the undersigned, understand that this Agreement describes my obligations to protect my electronic signature and password, and to notify appropriate authorities if it is stolen, lost, compromised, unaccounted for, or destroyed. I agree to the following terms and conditions:

I agree that my electronic signature will be valid for one year from date of issuance or earlier if it is revoked or terminated per the terms of this agreement. I will be notified and given the opportunity to renew my electronic signature each year prior to its expiration. The terms of this Agreement shall apply to each such renewal.

I will use my electronic signature and/or password to establish my identity and sign electronic documents and forms. I am solely responsible for protecting my electronic signature. If I suspect or discover that my electronic signature has been stolen, lost, used by an unauthorized party, or otherwise compromised, then I will immediately notify the HIPAA Security Designee at my site, Executive Director or his/her designee and request that my electronic signature be revoked. I will then immediately cease all use of my electronic signature. I agree to keep my electronic signature confidential and secure by taking reasonable security measures to prevent it from being lost, modified or otherwise compromised, and to prevent unauthorized disclosure of, access to, or use of it or of any media on which information about it is stored.

I will immediately request that my electronic signature be revoked if I discover or suspect that it has been or is in danger of being lost, disclosed, compromised or subjected to unauthorized use in any way. I understand that I may also request revocation at any time for any other reason.

If I have requested that my electronic signature be revoked, or I am notified that someone has requested that my electronic signature be suspended or revoked, and I suspect or discover that it has been or may be compromised or subjected to unauthorized use in any way, I will immediately cease using my electronic signature. I will also immediately cease using my electronic signature upon termination of employment or termination of this Agreement.

I further agree that, for the purposes of authorizing and authenticating electronic health records, my electronic signature and/or password has the full force and effect of a signature affixed by hand to a paper document and authenticity of the signature cannot be denied.

_____ _____

Employee Signature Date

_____

Employee Printed Name

APPENDIX A

Administrative Services Policies for Consumer Privacy

- Consumer Privacy Rights
- Designation of a Local HIPAA Representative
- Mandatory Breach Notification
- Minimum Necessary Uses, Disclosures, and Requests
- Notice of Privacy Practices
- Release of Information or Authorization to Release Information
- Release of Information to a Personal Representatives or Person Involved in a Consumer's Care
- Response to Subpoenas and Court Orders
- Uses and Disclosures of PHI for Marketing and Fundraising
- Workforce Agreement to Adhere to Privacy and Security Policies

APPENDIX B

Administrative Services Policies for Consumer Security

- Access Authorization, Establishment and Modification
- Acquisition and Decommissioning Leased/Owned Imaging Equipment
- Automatic Log-Off Policy
- Data Backup and Storage Policy
- Disposal of Protected Information
- Electronic Signature Policy
- Email Acceptable Use Policy
- Encryption and Decryption Policy
- Facility Security Policy
- Facsimile Transmission of PHI
- Hardware and Media Accountability Policy
- HIPAA Security Training Policy
- Information Systems Activity Review Policy
- Log-In Monitoring Policy
- Password Management Policy
- Record Retention and Destruction
- Security Incident Policy
- Security Reminders Policy
- Virus and Malware Protection Policy
- Workstation Use Policy

APPENDIX C

HIPAA Forms

- Acknowledgment of Receipt of Notice of Privacy Practices HF-06
- Spanish Edition HF-06s
- Authorization for Release/Receipt of Information HF-01
- Spanish Edition HF-01s
- Client PHI Privacy and Security Workforce Agreement HF-05
- Complaint Concerning Protected Health Information HF-02
- Spanish Edition HF-02s
- Request for Restriction on Manner of Confidential Communication HF-07
- Spanish Edition HF-07s
- Request Special Privacy Protections HF-04
- Spanish Edition HF-04s
- Request to Amend PHI HF-03
- Spanish Edition HF-03s

Documents

- Business Associate Agreement