

HIPAA Manual



Helping Others Soar

Victor Treatment Centers
Victor Community Support Services
2561 California Park Drive
Chico, CA

October 2011

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 Plan contains Victor'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 is comprised of residential treatment facilities, community-based programs, and non-public schools. Approximately 1,200 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 Privacy Officer serves under the direction of the Chief Executive Officer (CEO), 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 comprised of one representative from each program and 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 Plan 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 Chief Executive Officer (CEO), 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.
- Revise the HIPAA Compliance Plan periodically, in light of changes in the law.

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 Plan 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. When necessary to address a unique programmatic need, an individual program may, under the direction of the Agency's Privacy and Security Officers, make their policies and procedures stricter than those identified within.

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
- 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 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 the Privacy and Security Officers require corrective actions at the program level, the progress shall be monitored thoroughly 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 to sign annually the Workforce Agreement to Adhere to Privacy and Security Policies (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 Victor's 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.

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. 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 Officer 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 retribution or discipline for making good-faith reports of suspected non-compliance.

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](#)
- [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](#)