

Building Opportunities for Self-Sufficiency (BOSS) Notice of Privacy Practices

THIS NOTICE DESCRIBES HOW YOUR PROTECTED HEALTH INFORMATION, INCLUDING MEDICAL, MENTAL HEALTH, OR OTHER PROTECTED PERSONAL INFORMATION, 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 Privacy Notice, please contact a Program Director or our Privacy Officer at (510) 649-1931. The mailing address for our Privacy Officer is 2065 Kittredge, Ste. E, Berkeley, California, 94704.

I. OVERVIEW

A. INTRODUCTION

This notice describes Building Opportunities for Self-Sufficiency's privacy practices and those of all employees, staff, and other personnel who work for this agency and who are authorized to enter information into your client chart or have access to your Protected Health Information or Protected Personal Information at BOSS, including any student, intern or volunteer who might help you while you are here. These people all may share medical or mental health information about you with each other for purposes of treatment, payment, or operations as described in this notice.

B. PROTECTED HEALTH INFORMATION (PHI)

Protected Health Information means medical or mental health information we have collected from you or received from your health care providers or health plans. It may include information about your past, present or future physical or mental health care or condition, the provision of your health care, and payment for your health care services.

C. PROTECTED PERSONAL INFORMATION

Protected Personal Information is a subset of Protected Health Information and refers to information that can be used to identify you in the Alameda County Homeless Management Information System, also known as InHOUSE. As a recipient of federal homeless funding through the Alameda County Continuum of Care, BOSS is required to participate in the InHOUSE system for purposes of data collection and reporting on homeless services in Alameda County. Further information on the use of your Protected Personal Information in the InHOUSE system can be found in Section IV of this document.

D. BOSS'S RESPONSIBILITY

We understand that your medical and mental health information is personal and we are committed to protecting this information. We create a record of the care and services you receive at this agency so that we can provide you with quality care and comply with certain legal requirements. This notice applies to all of the records of your care that are generated by BOSS, its providers and staff, and those who provide services to you at BOSS.

E. WHAT THIS NOTICE TELLS YOU

This notice will tell you about the ways in which we may use and disclose medical or mental health information about you. It also describes your rights and certain obligations we have regarding the use and disclosure of your Protected Health Information. We are required by law to make sure the medical/mental health information that identifies you is kept private, to give you notice of our legal duties and privacy practices with respect to this information, and to follow the terms of the notice currently in effect.

II. HOW WE WILL USE AND DISCLOSE YOUR HEALTH INFORMATION

We will use and disclose your health information as described in each category listed below. For each category, we will explain what we mean in general, but not describe all specific uses or disclosures of health information. In this document, when we use the term health information, we will always be referring to protected health information, including both medical and mental health information, as well as other protected personal information.

A. USES AND DISCLOSURES FOR TREATMENT, PAYMENT AND OPERATIONS

1. For Treatment

We will use and disclose your health information without your authorization to provide your health care and any related services. For example, we may need to disclose information to a case manager who is responsible for coordinating your care.

We may disclose your health information among our clinical staff and other staff who work at BOSS. For example, our staff may discuss your care at a case conference.

We may also disclose your health information to qualified behavioral health care professionals at other agencies, clinics, services, laboratories or individual practitioner offices who are involved with your treatment.

Examples of other qualified behavioral and physical health care professionals include (but are not limited to): psychiatrists, psychologists, social workers, marriage and family therapists and registered interns, and other behavioral healthcare providers; medical doctors, nurses, medical students, dentists, and technicians.

For example, we may discuss how you are doing with your psychiatrist or therapist to coordinate treatment or talk about any concerns about medications.

We may also disclose information when a referral is made to a new provider.

2. For Payment

We may use or disclose your health information without your authorization so that the treatment and services you receive are billed to, and payment is collected from, your health plan or other third party payer. By way of example, we may disclose your health information to permit your health plan to take certain actions before your health plan approves or pays for your services.

- These actions may include: making a determination of eligibility or coverage for health insurance;
- reviewing your services to determine if they were medically necessary;
- reviewing your services to determine if they were appropriately authorized or certified in advance of your care; or
- reviewing your services for purposes of utilization review, to ensure the appropriateness of your care, or to justify the charges for your care.

For example, your health plan may ask us to share your Protected Health Information in order to approve additional length of stay in our program.

We may also disclose your Protected Health Information to another health care provider so that provider can bill you for services they provided to you, for example an ambulance service that transported you to the hospital.

3. For Health Care Operations

We may use and disclose health information about you without your authorization for our health care operations. These uses and disclosures are necessary to run our organization and make sure that our consumers receive quality care.

These activities may include, by way of example: quality assessment and improvement; reviewing the performance or qualifications of our clinicians; licensing and accreditation; training students in clinical activities; and general administrative activities.

We may combine health information of many of our clients to decide what additional services we should

offer, what services are no longer needed, and whether certain treatments are effective.

We may also provide your health information to other health care providers or to your health plan to assist them in performing certain of your own health care operations. We will do so only if you have or have had a relationship with the other provider or health plan.

We may also use and disclose your health information to contact you to remind you of your appointment.

Finally, we may use and disclose your health information to inform you about possible treatment options or alternatives that may be of interest to you.

4. Health-Related Benefits and Services

We may use and disclose health information to tell you about health-related benefits or services that may be of interest to you. For example, we may send you a notice of a health fair you may want to attend.

If you do not want us to provide you with information about health-related benefits or services, you must notify the Privacy Officer in writing at the address at the top of this notice. Please state clearly that you do not want to receive materials about health related benefits or services.

B. DISCLOSURES ONLY AFTER YOU HAVE BEEN GIVEN OPPORTUNITY TO OBJECT

There are situations where we will not share your health information unless we have discussed it with you (if possible) and you have not objected to this sharing.

These situations are:

1. Persons Involved in Your Care

In limited circumstances, we may disclose to a family member, a close personal friend, or another person that you have named as being involved in your health care (or the payment for your healthcare) your health information that is related to the person's involvement.

For example, if you ask a family member or friend to pick up a medication for you at the pharmacy we may tell that person what the medication is and when it will be ready. Also, we may notify a family member about your location and medical condition providing you do not object.

If you are physically present and have the capacity to make health care decisions, your health information may only be disclosed with your agreement to persons you designate to be involved in your care.

But, if you are in an emergency situation, we may disclose your health information to a spouse, a family member, or a friend so that such person may assist in your care.

In this case we will determine whether the disclosure is in your best interest and, if so, only disclose information that is directly relevant to participation in your care. And, if you are not in an emergency situation but are unable to make health care decisions, we will disclose your health information to:

- a person designated to participate in your care in accordance with an advance directive validly

executed under state law;

- your guardian if one has been appointed by a court, or, if applicable, the state agency responsible for consenting to your care. We may also disclose your health information to an entity assisting in disaster relief efforts and to coordinate disclosure for this purpose to family and other individuals involved in your care.

2. Sharing of your Protected Personal Information in the InHOUSE system

While BOSS is required to collect your Protected Personal Information for its data collection and reporting purposes, you have the right to limit what BOSS can share with other agencies that also participate in the InHOUSE system. Further information on your rights and the use of your Protected Personal Information in the InHOUSE system can be found in Attachment A of this document.

C. USES AND DISCLOSURES THAT MAY BE MADE WITHOUT YOUR AUTHORIZATION OR OPPORTUNITY TO OBJECT

1. Emergencies

We may use and disclose your health information in an emergency treatment situation. By way of example, we may provide your health information to a paramedic who is transporting you in an ambulance. If a clinician is required by law to treat you and your treating clinician has attempted to obtain your authorization but is unable to do so, the treating clinician may nevertheless use or disclose your health information to treat you.

2. Research

We may disclose your health information to researchers when your research has been approved by an Institutional Review Board or a similar privacy board that has reviewed the research proposal and established protocols to protect the privacy of your health information.

3. As Required By Law

We will disclose health information about you when required to do so by federal, state or local law.

4. To Avert a Serious Threat to Health or Safety

We may use and disclose health information about you when necessary to prevent a serious and imminent threat to your health or safety or to the health or safety of the public or another person. Under these circumstances, we will only disclose health information to someone who is able to help prevent or lessen the threat.

5. Public Health Activities

We may disclose health information about you as necessary for public health activities including, by way of example, disclosures to:

- notify the appropriate government agency if we believe you have been a victim of abuse, neglect

or domestic violence. We will only notify an agency if we obtain your agreement or if we are required or authorized by law to report such abuse, neglect or domestic violence.

- report to public health authorities for the purpose of preventing or controlling disease, injury or disability;
- report vital events such as birth or death;
- conduct public health surveillance or investigations;
- report child, elder, or dependent abuse or neglect;
- report certain events to the Food and Drug Administration (FDA) or to a person subject to the jurisdiction of the FDA including information about defective products or problems with medications;
- notify consumers about FDA-initiated product recalls;
- notify a person who may have been exposed to a communicable disease or who is at risk of contracting or spreading a disease or condition.

6. Health Oversight Activities

We may disclose health information about you to a health oversight agency for activities authorized by law.

Oversight agencies include government agencies that oversee the health care system, government benefit programs such as Medicare or Medicaid, other government programs regulating health care, and civil rights laws.

7. Disclosures in Legal Proceedings

We may disclose health information about you to a court or administrative agency when a judge or administrative agency orders us to do so.

We also may disclose health information about you in legal proceedings without your permission or without a judge or administrative agency's order when we receive a subpoena for your health information.

We will not provide this information in response to a subpoena without your authorization unless we are ordered to do so by the court.

8. Law Enforcement Activities

We may disclose health information to a law enforcement official for law enforcement purposes when:

- a court order, subpoena, warrant, summons or similar process requires us to do so; or
- the information is needed to identify or locate a suspect, fugitive, material witness or missing person; or
- we report a death that we believe may be the result of criminal conduct; or
- we report criminal conduct occurring on the premises of our facility; or
- we determine that the law enforcement purpose is to respond to a threat of an imminently

dangerous activity by you against yourself or another person; or

- the disclosure is otherwise required by law.

We may also disclose health information about a client who is a victim of a crime, without a court order or without being required to do so by law. However, we will do so only if the disclosure has been requested by a law enforcement official and the victim agrees to the disclosure or, in the case of the victim's capacity, the following occurs:

- the law enforcement official represents to us that:
 - the victim is not the subject of the investigation, and
 - an immediate law enforcement activity to meet a serious danger to the victim or others depends upon the disclosure; and
- we determine that the disclosure is in the victim's best interest.

9. Medical Examiners or Funeral Directors

We may provide health information about our consumers to a medical examiner. Medical examiners are appointed by law to assist in identifying deceased persons and to determine the cause of death in certain circumstances. We may also disclose health information about our consumers to funeral directors as necessary to carry out your duties.

10. Military and Veterans

We may disclose your health information for the purpose of determining your eligibility for benefits provided by the Department of Veterans Affairs.

11. National Security and Protective Services for the President and Others

We may disclose medical information about you to authorized federal officials for intelligence, counter-intelligence, and other national security activities authorized by law.

We may also disclose health information about you to authorized federal officials so they may provide protection to the President, other authorized persons or foreign heads of state or so they may conduct special investigations.

12. Inmates

If you are an inmate of a correctional institution or under the custody of a law enforcement official, we may disclose health information about you to the correctional institution or law enforcement official.

13. Workers' Compensation

We may disclose health information about you to comply with the state's Workers' Compensation Law.

14. Uses and Disclosures of Your Health Information with Your Permission

Uses and disclosures not described in this Notice of Privacy Practices will generally only be made with

your written permission, called an authorization.

You have the right to revoke an authorization at any time. If you revoke your authorization we will not make any further uses or disclosures of your health information under that authorization, unless we have already taken an action relying upon the uses or disclosures you have previously authorized.

III. YOUR RIGHTS REGARDING YOUR HEALTH INFORMATION.

A. RIGHT TO INSPECT AND COPY

You have the right to request an opportunity to inspect or copy health information used to make decisions about your care, whether they are decisions about your treatment or payment of your care. Usually, this would include clinical and billing records, but not psychotherapy notes.

You must submit your request in writing to our Privacy Officer at BOSS, 2065 Kittredge, Suite E, Berkeley, California, 94704.

If you request a copy of the information, we may charge a fee for the cost of copying, mailing and supplies associated with your request.

We may deny your request to inspect or copy your health information in certain limited circumstances. In some cases, you will have the right to have the denial reviewed by a licensed health care professional not directly involved in the original decision to deny access.

We will inform you in writing if the denial of your request may be reviewed. Once the review is completed, we will honor the decision made by the licensed health care professional reviewer.

B. RIGHT TO AMEND

For as long as we keep records about you, you have the right to request us to amend any health information used to make decisions about your care whether they are decisions about your treatment or payment of your care. Usually, this would include clinical and billing records, but not psychotherapy notes.

To request an amendment, you must submit a written document to our Privacy Officer at BOSS, 2065 Kittredge, Suite E, Berkeley, California, 94704 and tell us why you believe the information is correct or inaccurate.

We may deny your request for an amendment if it is not in writing or does not include a reason to support the request. We may also deny your request if you ask us to amend health information that:

- was not created by us, unless the person or entity that created the health information is no longer available to make the amendment;
- is not part of the health information we maintain to make decisions about your care;
- is not part of the health information that you would be permitted to inspect or copy; or
- is accurate and complete.

If we deny your request to amend, we will send you a written notice of the denial stating the basis for the denial and offering you the opportunity to provide a written statement disagreeing with the denial.

If you do not wish to prepare a written statement of disagreement, you may ask that the requested amendment and our denial be attached to all future disclosures of the health information that is the subject of your request.

If you choose to submit a written statement of disagreement, we have the right to prepare a written rebuttal to your statement of disagreement. In this case, we will attach the written request and the rebuttal (as well as the original request and denial) to all future disclosures of the health information that is the subject of your request.

C. RIGHT TO AN ACCOUNTING OF DISCLOSURES

You have the right to request that we provide you with an accounting of disclosures we have made of your health information. An accounting is a list of disclosures.

But this list will not include certain disclosures of your health information, by way of example, those we have made for purposes of treatment, payment, and health care operations.

To request an accounting of disclosures, you must submit your request in writing to the Privacy Officer at BOSS, 2065 Kittredge, Suite E, Berkeley, California, 94704.

For your convenience, you may submit your request on a form called a Request For Accounting, which you may obtain from our Privacy Officer.

The request should state the time period for which you wish to receive an accounting. This time period should not be longer than six years and not include dates before April 14, 2003.

The first accounting you request within a twelve month period will be free. For additional requests during the same 12-month period, we will charge you for the costs of providing the accounting. We will notify you of the amount we will charge and you may choose to withdraw or modify your request before we incur any costs.

D. RIGHT TO REQUEST RESTRICTIONS

You have the right to request a restriction on the health information we use or disclose about you for treatment, payment or health care operations.

To request a restriction, you must request the restriction in writing addressed to the Privacy Officer at Privacy Officer at BOSS, 2065 Kittredge, Suite E, Berkeley, California, 94704.

The Privacy Officer will ask you to sign a request for restriction form, which you should complete and return to the Privacy Officer.

We are not required to agree to a restriction that you may request. If we do agree, we will honor your request unless the restricted health information is needed to provide you with emergency treatment.

E. RIGHT TO REQUEST CONFIDENTIAL COMMUNICATIONS

You have the right to request that we communicate with you about your health care only in a certain location or through a certain method.

For example, you may request that we contact you by leaving messages only at a specific number or sending you mail only to a specific address.

To request such a confidential communication, you must make your request in writing to the Privacy Officer at BOSS, 2065 Kittredge, Suite E, Berkeley, California, 94704.

We will accommodate all reasonable requests.

You do not need to give us a reason for the request; but your request must specify how or where you wish to be contacted.

F. RIGHT TO A PAPER COPY OF THIS NOTICE

You have the right to obtain a paper copy of this Notice of Privacy Practices at any time.

Even if you have agreed to receive this Notice of Privacy Practices electronically, you may still obtain a paper copy.

To obtain a paper copy, contact our Privacy Officer at Privacy Officer at BOSS, 2065 Kittredge, Suite E, Berkeley, California, 94704.

IV. PRIVACY AND CONFIDENTIALITY IN THE ALAMEDA COUNTY HOMELESS MANAGEMENT INFORMATION SYSTEM (INHOUSE)

A. PURPOSE OF THIS SECTION

As a recipient of federal homeless funding through the Alameda County Continuum of Care, BOSS is required to participate in the InHOUSE system for purposes of data collection and reporting on homeless services in Alameda County. Protected Personal Information is a subset of Protected Health Information and refers to information that can be used to identify you in the Alameda County Homeless Management Information System, also known as InHOUSE. The purpose of this section is to describe the uses of your Protected Personal Information in the InHOUSE system, the procedures used to protect that information, and your rights regarding the use of your information in the InHOUSE system.

B. STATEMENT OF POLICY

BOSS will comply with all applicable laws governing Homeless Management Information System client privacy and confidentiality. Applicable standards include, but are not limited to the following:

- Federal Register Vol. 69, No. 146 (I IMIS FR 4848 N 02) Federal statute governing HMIS

information Friday, July 30, 2004.

- HIPAA the Health Insurance Portability Act.
- 42 CFR Part 2. Federal statute governing drug and alcohol treatment.
- Alameda County wide Continuum of Care InHOUSE Policy and Procedures manual.
- Alameda County wide Continuum of Care InHOUSE partner agency sharing agreement(s).

C. USE OF INFORMATION

Protected Personal Information is information which can be used to identify you as a specific client and can be used only for the following purposes:

- To provide or coordinate services for you.
- For functions related to payment or reimbursement for services provided to you.
- To carry out administrative functions such as legal, audit, personnel planning, oversight and management functions.
- For creating de-personalized identification for unduplicated counting.
- Where disclosure is required by law.
- To prevent or lessen a serious and imminent threat to the health or safety of an individual or the public.
- To report abuse, neglect, or domestic violence as required or allowed by law.
- Contractual research where privacy conditions are met (including a written agreement).
- To report criminal activity on agency premises.
- For law enforcement purposes in response to a properly authorized request for information from a properly authorized source.

D. COLLECTION AND NOTIFICATION

Information will be collected only by fair and lawful means with your knowledge or consent.

- Protected Personal Information will be collected only for the purposes listed above.
- You and all other clients will be made aware that personal information is being collected and recorded and will be asked to express written consent to have your information entered in the InHOUSE system.
- A written sign will be posted in locations where Protected Personal Information is collected. This written notice will read:

"We collect personal information directly from you for reasons that are discussed in our Privacy Notice. We may be required to collect some personal information by law or by organizations that give us money to operate this program. Other personal information that we collect is important to run our programs, to improve services for homeless persons, and to better understand the needs of homeless persons. We only collect information that we consider to be appropriate.

The collection and use of all personal information is guided by strict standards of confidentiality. Our Privacy Notice is posted. A copy of our Privacy Notice will be made available to you and all

other clients upon request."

- Staff will explain the sign if a client is unable to read or understand it.

E. DATA QUALITY

Protected Personal Information data will be accurate, complete, timely, and relevant.

- All Protected Personal Information collected will be relevant to the purposes for which it is to be used.
- Identifiers will be removed from data that is not in current use after 7 years (from date of creation or last edit) unless other requirements mandate longer retention.
- Data will be entered in a consistent manner by authorized users.
- Data will be entered in as close to real-time data entry as possible.
- Measures will be developed to monitor data for accuracy and completeness and for the correction of errors.
 - The agency runs reports and queries monthly to help identify incomplete or inaccurate information.
 - The agency monitors the correction of incomplete or inaccurate information.
 - By the 15th of the following month all monitoring reports will reflect corrected data.
- Data quality is subject to routine audit by System Administrators who have administrative responsibilities for the database.

F. PRIVACY NOTICE, PURPOSE SPECIFICATION AND USE LIMITATIONS

The purposes for collecting Protected Personal Information data, as well as its uses and disclosures will be specified and limited.

- The purposes, uses, disclosures, policies, and practices relative to Protected Personal Information data are to be outlined in this agency Privacy Notice.
- The agency Privacy Notice will comply with all applicable regulatory and contractual limitations.
- The agency Privacy Notice will be made available to you, or your representative, upon request and explained/interpreted as needed.
- Reasonable accommodations will be made with regards to the Privacy Notice for persons with disabilities and non-English speaking clients as required by law.
- Protected Personal Information will be used and disclosed only as specified in the Privacy Notice, and only for the purposes specified therein.
- Uses and disclosures not specified in the Privacy Notice can be made only with your consent.
- The Privacy Notice will be posted on the agency web site.
- The Privacy Notice will be reviewed and amended as needed.
- Amendments to or revisions of the Privacy Notice will address the retroactivity of any changes.
- Permanent documentation will be maintained of all Privacy Notice amendments/revisions.

- All access to, and editing of Protected Personal Information data will be tracked by an automated audit trail, and will be monitored for violations use/disclosure limitations.

G. RECORD ACCESS AND CORRECTION

Provisions will be maintained for the access to and corrections of Protected Personal Information records.

- You will be allowed to review your InHOUSE record within 5 working days of a request to do so.
- During a review of your record, an agency staff person must be available to explain any entries that you do not understand.
- You may request to have your record corrected so that information is up-to-date and accurate to ensure fairness in its use.
- When a correction is requested by you, the request will be documented and the staff will make a corrective entry if the request is valid.
- You may be denied access to your personal information for the following reasons:
 - Information is compiled in reasonable anticipation of litigation or comparable proceedings.
 - Information about another individual other than the agency staff would be disclosed.
 - Information was obtained under a promise of confidentiality other than a promise from this provider and disclosure would reveal the source of the information.
 - Information, the disclosure of which would be reasonably likely to endanger the life or physical safety of any individual.
- In the case of repeated or harassing requests for access or correction. However, if denied, documentation will be provided regarding the request and reason for denial to the individual and be made a part of the client's record.

H. ACCOUNTABILITY

Processes will be maintained to ensure that the privacy and confidentiality of your Protected Personal Information is protected and staff is properly prepared and accountable to carry out agency policies and procedure that govern the use of Protected Personal Information data.

- Grievances may be initiated through the agency privacy grievance process for considering questions or complaints regarding privacy and security policies and practices. All users of the InHOUSE system must sign a Users Agreement that specifies each staff persons'™ obligations with regard to protecting the privacy of Protected Personal Information and indicates that they have received a copy of the agency's Privacy Notice and that they will comply with its guidelines.
- All users of the InHOUSE system must complete formal privacy training.
- A process will be maintained to document and verify completion of training requirements.
- A process will be maintained to monitor and audit compliance with basic privacy requirements including but not limited to auditing clients entered against signed InHOUSE Consent Releases. At minimum, a quarterly Compliance Review will be conducted and documented.
- A copy of any staff grievances initiated relative to privacy, confidentiality, or InHOUSE system data will be forwarded to Continuum of Care Staff.

- Regular user meetings will be held and issues concerning data security, client confidentiality, and information privacy will be discussed and solutions will be developed.
- A grievance process may be initiated if you feel that your confidentiality rights have been violated, if access has been denied to your personal records, or if they have been put at personal risk, or harmed.
- Any grievances you may file relative to the InHOUSE system will be processed and resolved according to agency's privacy grievance policy.
- If you are unsatisfied with the resolution of your grievance at the agency level, you may request mediation at the system level.

I. SHARING OF INFORMATION

Your Protected Personal Information may be shared with partnering agencies only with your approval.

- All routine data sharing practices with partnering agencies will be documented and governed by the Continuum of Care Memorandum of Understanding Agreement that defines the agency-determined sharing practice.
- A completed InHOUSE Client Release of Information Form is needed before information may be shared electronically.
 - The InHOUSE Release of Information Form is to inform you about what is shared and with whom it is shared.
 - You have the right to either accept or reject the sharing plan, and you may select the extent of sharing.
 - If you reject the sharing plan, staff will click the Security Button, which closes the record.
 - If you select collaborative sharing only, the record is closed with designated exceptions.
- You will be informed about and understand the benefits, risks, and available alternatives to sharing your information prior to signing a Release of Information Form, and your decision to grant permission shall be voluntary.
- If you choose not to authorize sharing of information you cannot be denied services for which you would otherwise be eligible.
- All Client Authorization for Release of Information forms related to the InHOUSE system will be placed in a file to be located on premises and will be made available to the Continuum of Care Staff for periodic audits.
- InHOUSE-related Authorization for Release of Information forms will be retained for a minimum period of three (3) years, after which time the forms will be discarded in a manner that ensures client confidentiality is not compromised.
- No confidential/restricted information received from the InHOUSE system will be shared with any organization or individual without proper written consent by the client, unless otherwise permitted by applicable regulations or laws.
- Restricted information, including progress notes and psychotherapy notes about the diagnosis, treatment, or referrals related to a medical health, disabilities, mental health disorder, drug or alcohol use, HIV/AIDS, and any violence-related concerns shall not be shared with other participating Agencies without the clients written, informed consent as documented on the Agency

Authorization for Release of Restricted Information Form.

- Sharing of restricted information is not covered under the general InHOUSE Client Release of Information.
- Sharing of restricted information must also be planned and documented through a fully executed Authorization for Release of Restricted Information Form
- If a field that normally contains non-confidential information discloses confidential information.
 - The staff completes an Authorization for Release of Restricted Information Form.
 - If you refuse to authorize the release, the staff closes the Assessment/Screen by clicking the lock on the screen and removing any exceptions.
- If you have previously given permission to share information with multiple agencies, beyond basic identifying information and non-restricted service transactions, and then choose to revoke that permission with regard to one or more of these agencies, the affected agency/ agencies will be contacted accordingly, and those portions of the record impacted by the revocation, too will be locked from further sharing.
- All Release of Information forms will include an expiration date, and once a Release of Information expires, any new information entered will be closed to sharing unless a new Release of Information Form is signed by you and entered in the InHOUSE system.

J. SYSTEM SECURITY

System security provisions will apply to all systems where Protected Personal Information is stored: agency's networks, desktops, laptops, mini-computers, mainframes and servers.

- Password Access
 - Only individuals who have completed Privacy and System Training may be given access to the InHOUSE system through User IDs and Passwords,
 - Temporary default passwords will be changed on first use.
 - Access to Protected Personal Information requires a user name and password at least 8 characters long and using at least one number and one letter.
 - Passwords will not use or include the users name or the vendor name, and will not consist entirely of any word found in the common dictionary or any of the above words spelled backwards.
 - User Name and password may not be stored or displayed in any publicly accessible location.
 - Passwords must be changed routinely.
 - Users must not be able to log onto more than one workstation or location at a time.
 - Individuals with User IDs and Passwords will not give or share assigned User IDs and Passwords to access the InHOUSE system with any other person, organization, governmental entity, business.
- Virus Protection and Firewalls:
 - Commercial anti-virus protection software will maintained to protect all agency network systems and workstations from virus attack.

- Virus protection will include automated scanning of files as they are accessed by users.
- Virus Definitions will be updated regularly.
- All workstations will be protected by a firewall either through a workstation firewall or a server firewall.
- Physical Access to Systems where InHOUSE Data is Stored
 - Computers stationed in public places must be secured when workstations are not in use and staff is not present.
 - After a short period of time a pass word protected screen saver will be activated during time that the system is temporarily not in use.
 - For extended absence from a workstation, staff must log off the computer.
- Stored Data Security and Disposal:
 - All InHOUSE data downloaded onto a data storage medium must be maintained and stored in a secure location, not accessible to non-licensed users of the InHOUSE system.
 - Data containing Protected Personal Information will not be downloaded to any remote access site at any time for any reason, nor transmitted outside the physical agency by any means whatsoever.
 - Data stored on a portable medium will be secured when not in use and will never be taken off site at any time for any reason.
 - Data downloaded for purposes of statistical analysis will exclude Protected Personal Information whenever possible.
 - InHOUSE data downloaded onto a data storage medium must be disposed of by reformatting as opposed to erasing or deleting. This includes hard drives.
 - A data storage medium will be reformatted a second time before the medium is reused or disposed of.
- System Monitoring
 - User access to the InHOUSE Live Web Site will be monitored using the computer access logs located on each computer's explorer "history" button, or via a central server report.
- Hard Copy Security:
 - Any paper or other hard copy containing Protected Personal Information that is either generated by or for InHOUSE including, but not limited to report, data entry forms and signed consent forms will be secured.
 - Agency staff will supervise at all time hard copy with identifying information generated by or for the InHOUSE system when the hard copy is in a public area. If the staff leaves the area, the hard copy must be secured in areas not accessible by the public.
 - All written information pertaining to the user name and password must not be stored or displayed in any public accessible location.
- Authorized Location Access:
 - Access to the InHOUSE system is allowed only from authorized agency locations.

K. AGENCY GRIEVANCE POLICY FOR INHOUSE SYSTEM

If you have a problem, concern or complaint regarding the use of your Protected Personal Information in the InHOUSE System you should follow these steps:

- Step 1: Attempt to resolve the problem at the program level with the program supervisor. If not resolved, then
- Step 2: Attempt to resolve the problem at the agency level by filing a written complaint with the BOSS Privacy Officer. If not resolved, then
- Step 3: You have recourse to resolution of your grievance regarding your Protected Personal Information and the InHOUSE System through mediation provided by the Alameda County Continuum of Care.

At all steps, our Privacy Officer, who can be contacted at BOSS, 2065 Kittredge, Suite E, Berkeley, California, 94704, will assist you with writing your complaint, if you request such assistance.

We will not retaliate against you for filing a complaint or grievance.

L. ALL OTHER PRIVACY COMPLAINTS

If you believe your privacy rights have been violated, you may file a complaint with us or with the Secretary of the U.S. Department of Health and Human Services.

To file a complaint with us, contact our office responsible for receiving complaints at the Privacy Officer at BOSS, 2065 Kittredge, Suite E, Berkeley, California, 94704.

All complaints must be submitted in writing.

Our Privacy Officer, who can be contacted at BOSS, 2065 Kittredge, Suite E, Berkeley, California, 94704 will assist you with writing your complaint, if you request such assistance.

We will not retaliate against you for filing a complaint.

V. CHANGES TO THIS NOTICE

We reserve the right to change the terms of our Notice of Privacy Practices. We also reserve the right to make the revised or changed Notice of Privacy Practices effective for all health information we already have about you as well as any health information we receive in the future.

We will post a copy of the current Notice of Privacy Practices at our main office and at each site where we provide care.

You may also obtain a copy of the current Notice of Privacy Practices by accessing our website at www.self-sufficiency.org or by calling us at (510) 649-8174 and requesting that a copy be sent to you in the mail or by asking for one any time you are at our offices.

Building Opportunities for Self-Sufficiency (BOSS)
[NOTICE OF PRIVACY PRACTICES Revised June 2005]