

SF DPH PRIVACY/HIPAA POLICIES - IMPLEMENTATION CHECKLIST (7/07)

1.0	The DPH Privacy Policy is integrated in the program's governing policies and procedures regarding patient privacy and confidentiality.
1.01	Make readily accessible to staff a Compliance Binder containing the agency's Code of Conduct and HIPAA Privacy Policies and Procedures.
1.02	Distribute the "DPH Privacy Policy Matrix - Sharing Patient Health Information Between Treatment Providers" to provider staff.
1.03	Include only limited information on the client/patient sign-in sheets and schedules.
1.04	As appropriate, call clients/patients by first name only.
1.05	Keep voices low when discussing PHI.
1.06	Avoid discussing PHI in elevators or hallways where unauthorized disclosure could accidentally occur.
1.07	Use private rooms whenever possible.
1.08	Turn medical charts face down on desks, counters, and in chart holders.
1.09	Keep medical records in a locked drawer or cabinet located in a central file area at the end of the day.
1.10	Turn computer monitors away from the view of unauthorized persons.
1.11	Lock computers when unattended, to prevent unauthorized access.
1.12	Locate faxes, copiers, and printers in secure areas.
1.13	Establish policies and procedures for record storage and destruction.
1.14	Shred unneeded documents containing PHI in a confidential destruction bin.
1.15	Screening / Triage / Interviewing of clients/patients is private and <u>cannot</u> be heard by other patients (e.g., conducted in common areas such as waiting rooms or in spaces where private conversations can be easily heard by others).

2.0	All staff who handle patient health information are oriented and trained in the program's privacy/confidentiality policies and procedures.
2.01	Provide HIPAA / Privacy Awareness training to staff who have access to PHI.
2.02	Document HIPAA / Privacy Awareness training complete with staff's printed name, signature, trainer name, and date of training.
2.03	Provide job-specific HIPAA / Privacy training, including the use of HIPAA Privacy Forms, to staff who have access to PHI.
2.04	Document job-specific HIPAA / Privacy training complete with staff's printed name, signature, trainer name, and date of training.
2.05	Communicate privacy expectations and reminders to staff by email and at staff meetings.
2.06	Implement disciplinary procedures and document disciplinary action taken, when staff violate the program's privacy policies and procedures.

3.0	A Privacy Notice that meets the requirements of the Federal Privacy Rule (HIPAA) is written and provided to all patients/clients served in their threshold and other languages. If the document is not available in the patient's/client's relevant language, verbal translation is provided.
3.01	Always have available a sufficient supply of HIPAA Privacy forms. For DPH programs, forms are available on http://www.dph.sf.ca.us/InsideDPH/HIPAA/HIPAAsumNotice.htm#HIPAA
	a) (Detailed) Notice of Privacy Practices in threshold and other languages (attached)
	b) Summary Notice of HIPAA Privacy Practices and Acknowledgment Form in threshold and other languages
	c) Authorization for Release of Patient Information
	d) Request for Accounting of Disclosures

SF DPH PRIVACY/HIPAA POLICIES - IMPLEMENTATION CHECKLIST (7/07)

3.0	A Privacy Notice that meets the requirements of the Federal Privacy Rule (HIPAA) is written and provided to all patients/clients served in their threshold and other languages. If the document is not available in the patient's/client's relevant language, verbal translation is provided.
	e) Request to Amend Medical Record
	f) Release of Information Authorization for Psychotherapy Notes
	g) Medical Record Disclosure Log
3.02	Review the medical records (in any medium) of each day's appointment, to determine if a HIPAA Privacy Notice has been provided to the clients/patients who are scheduled to be seen on that day.
3.03	If the client/patient has not been noticed, ensure that a full Notice, and a Summary and Acknowledgement Form are provided to him/her during the appointment.
3.04	Explain the Summary Notice to the client/patient, and ask him/her to sign the Acknowledgement form.
3.05	If the client/patient refuses to sign the Acknowledgment form, document the refusal on the form, sign your name, and date it.
3.06	If the client/patient speaks only a language into which the Privacy Notice and Summary and Acknowledgment form has <u>not</u> been translated, obtain interpreter service for him/her.
3.07	Document that interpreter service was provided, in the client/patient's medical records. Have client/patient sign the acknowledgement form, and follow usual procedures.

4.0	A Summary of the Privacy Notice is posted and visible in registration and common areas of treatment facility.
4.01	Place the HIPAA Summary Notice or Poster in a common area that is highly visible to clients/patients.
4.02	Place Privacy Photo Posters in high traffic areas throughout the clinic or program site.

5.0	Each disclosure of a patient's health information for purposes other than treatment, payment, or operations is documented.
5.01	Document requests for confidential communication in the medical records.
5.02	Confirm the identity and fax numbers of the recipient prior to sending PHI.
5.03	Keep a log of non-routine PHI disclosures. Include the name and address of the requestor, relation to patient, brief description of PHI provided, name of staff who provided the PHI, and the date, time, and how PHI was provided.

6.0	Authorization for disclosure of a patient's health information is obtained prior to release as required; that is (1) to providers outside the DPH Safety Net and (2) from a substance abuse program.
6.01	Assure that Authorization forms meet HIPAA Privacy Rule requirements.
6.02	Do not combine "consent for treatment" with "authorization for disclosure" on the same form. As a general rule, do not use compound authorizations.
6.03	Do not deny treatment on the basis of the patient's refusal to authorize the use or disclosure of his PHI.
6.04	Write the authorization in plain language in 14 point font. It must include at a minimum: <ul style="list-style-type: none"> a) a description of the information to be used or disclosed; b) the name and address of the person or entity to whom the information will be disclosed; c) the purpose or use of the disclosure; d) the name of the person authorized to make the disclosure;

SF DPH PRIVACY/HIPAA POLICIES - IMPLEMENTATION CHECKLIST (7/07)

6.0	Authorization for disclosure of a patient's health information is obtained prior to release as required; that is (1) to providers outside the DPH Safety Net and (2) from a substance abuse program.
	e) the signature of the individual or representative who is making the disclosure;
	f) the date of disclosure;
	g) the expiration date for the authorization; and
	h) statements that the individual has the right to proactively (not retroactively) revoke the authorization in writing, that DPH cannot condition treatment on the authorization, the consequence of refusal to sign the authorization, and the potential for re-disclosure (if any).
6.05	Provide a copy of the authorization to the patient.
6.06	File patient authorizations for release of PHI in the client/patient's medical records.
6.07	Retain patient authorizations in the patient files for at least 7 years.

7.0	Ensure that Protected Health Information (PHI) is transmitted in a secure manner.
7.01	For voice transmissions:
	a) Always confirm the voice mailbox as the intended recipient of PHI.
	b) Do not use voicemail to communicate PHI, unless deemed in the interest of the patient.
	c) Do not use voicemail to communicate PHI to the patient, unless the patient has signed a specific request or authorization.
	d) When using cell phones to disclose PHI, take care to call from areas where PHI cannot be inappropriately or unlawfully disclosed.
7.02	For email and fax transmissions:
	a) Always send PHI to confirmed electronic mail addresses or fax numbers only, not to distribution lists.
	b) For routine transmission of PHI via fax, program numbers into fax machine to minimize the potential for error. Check these numbers periodically to ensure that they are valid.
	c) Always include a confidentiality message in all electronic mail transmissions and fax cover sheets, such as "This message and any attachments are solely for the intended recipient and may contain confidential or privileged information. If you are not the intended recipient, any disclosure, copying, use, or distribution of the information included in this message and any attachments is prohibited. If you have received this communication in error, please notify me by reply e-mail and immediately and permanently delete this message and any attachments. Thank you."
	d) Limit PHI that is sent via fax or to electronic mail addresses, to the minimum necessary to perform the intended task.
	e) If it is determined that an electronic mail address is unsecured, or if the security of the electronic mail address cannot be verified, transmit PHI in password-protected files only. Send passwords to access the protected files, via a separate message.
	f) Use electronic mail to communicate with patients, but not to respond to requests for copies of medical records.
	g) Whenever a patient needs a copy of his or her medical records, always obtain a signed written authorization from the patient. After the provider determines that release of the information will not cause serious harm to the patient, a hard copy of the records may be released to the patient.
7.03	For wireless and infrared transmission:
	a) Transmit PHI only from approved portable computing devices and access points.
	b) Actuate the portable devices in secure environments only.
7.04	In case of inappropriate or insecure transmission, notify your supervisor immediately.

SF DPH PRIVACY/HIPAA POLICIES - IMPLEMENTATION CHECKLIST (7/07)

8.0	Observe the Privacy Rule for PHI release to the media.
8.01	Do not release information about mental health or substance abuse patients including their presence in the facility.
8.02	If a patient has not requested that information be withheld, you may release the medical condition of an inpatient, outpatient, or emergency patient to the media, but only if the inquiry specifically contains the patient's name. At the DPH, refer all media inquiries to the DPH Media Relations staff and /or to the Hospital Administrator on Duty,
8.03	Describe a patient's condition only in general terms that do not communicate specific medical information about the individual (eg., undetermined, good, fair, serious, critical or deceased).
8.04	Do not disclose additional information about a patient's death, including the cause, date, or time of death, without written authorization from a legal representative of the deceased patient, even if this information has been disclosed to the medical examiner or death registrar,