**Attachment B:**

**Notice of Privacy Practices Checklist**

## THE USES AND DISCLOSURES STATE ENTITY WILL MAKE OF A PATIENT’S HEALTH INFORMATION

1. THE NOTICE MUST CONTAIN:

* **Plain Language:** The notice must be written in plain language.
* **Header:** The notice must contain the following statement as a header or otherwise prominently displayed:

“*THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY*.”

* **Electronic Notice:** A covered entity that maintains a web site that provides information about the covered entity's customer services or benefits must prominently post its notice on the web site and make the notice available electronically through the web site.

1. EXAMPLES OF USES AND DISCLOSURES OF HEALTH INFORMATION

The notice must describe the following descriptions and examples of uses and disclosures:

* **Treatment**
* **Payment**
* **Healthcare Operations.** A description, including at least one example for each, that PHI may be used or disclosed for treatment, payment and healthcare operations.

1. NOTE TO AGENCIES THAT PARTNER WITH BUSINESS ASSOCIATES

A statement that certain companies ("business associates") that provide various services to the agency or organization (for example, billing, transcription, software maintenance, legal services, and managed care support) are required by law to protect a patient’s PHI and comply with the same HIPAA Privacy standards of the agency or organization.

The following information is meant to be a guide while developing, or revising your Notice of Privacy Practices. Please tailor the Notice of Privacy Practices to your specific needs (*ensuring that you include the mandatory components*).

1. **Persons Involved in the Patient’s Care.** A description that PHI may be used or disclosed to a family member, relative, close personal friend of the patient, or any other person identified by the patient for involvement in the patient’s care or payment related to the patient’s health care or for notification purposes.
2. **Disclosures about a decedent to family members and others involved in care.** If the patient is deceased, a covered entity may disclose to a family member, or certain other persons who were involved in the patient’s care or payment for health care prior to the patient’s death, protected health information of the patient that is relevant to such person’s involvement, unless doing so is inconsistent with any prior expressed preference of the patient that is known to the covered entity.
3. **[Optional] Opportunity to Object.** A description that the patient may object to this use or disclosure.
4. **Disaster Relief Purposes.** A description that the PHI may be used or disclosed to a public or private entity authorized by law or by its charter to assist in disaster relief efforts for the purpose of coordinating disaster relief efforts.
5. **Required by Law.** A description that PHI may be used or disclosed as required by law. Specific examples are recommended.
6. **Public Health Activities**. A description that PHI may be used or disclosed for public health activities. Explain the different categories of public health activities. Examples can include public health investigations, reporting of child abuse and neglect, FDA reporting, workplace medical surveillance, etc.
7. **Victims of Abuse, Neglect or Domestic Violence.** A description that PHI may be disclosed to a government authority about a patient whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence.
8. **[Optional] Informing the Patient.** A statement that the covered entity generally will inform the patient that such a report of suspected abuse, neglect, or domestic violence has been or will be made.
9. **Health Oversight Activities.** A description that PHI may be used or disclosed to a health oversight agency for health oversight activities authorized by law. Include brief explanation of what activities are considered health oversight activities.
10. **Judicial and Administrative Proceedings.** A description that PHI may be disclosed in the course of a judicial or administrative proceeding (court orders or subpoenas) only after required by law procedures are followed.
11. **Law Enforcement.** A description that PHI may be disclosed to a law enforcement official for law enforcement activities including correctional institutions[[1]](#footnote-1).
12. **Disclosures to Coroners, Medical Examiners and Funeral Directors.** A description that limited PHI may be used for purposes of identifying a deceased person, determining the cause of death, or other duties as authorized by law and for funeral directors as necessary to carry out their duties.
13. **Cadaveric Organ, Eye or Tissue Donation.** A description that PHI may be used or disclosed to cadaveric organ procurement, banking or transplantation organizations for the purpose of facilitating organ, eye, or tissue donation and transplantation.
14. **Research. A description that PHI may be used or disclosed for research purposes. [**Note, the covered entity may want to explain that uses and disclosures for research generally: require the patient’s authorization; require a decision by an institutional review board or privacy board that authorization is not necessary because the research involves no more than a minimal risk to the privacy of the research subjects; involve information that is mostly anonymous and is subject to a data use agreement; or are used solely to prepare a research protocol.]
15. **To Avert a Threat to Health or Safety.** A description that PHI may be used or disclosed to avert serious threats to the health or safety of a person or the public.
16. **Armed Forces and Military Personnel.** A description that PHI about patients who are Armed Forces personnel or foreign military personnel may be used or disclosed for activities deemed necessary by appropriate military command authorities.

*There are additional permissible uses and disclosures for covered entities that are components of the Departments of Defense, Transportation, Veterans Affairs, or State.*

1. **National Security and Intelligence Activities.** A description that PHI may be disclosed to authorized federal officials for the conduct of authorized intelligence, counter-intelligence and other national security activities.
2. **Protective Services for the President and Others.** A description that PHI may be disclosed to authorized federal officials for the provision of protective services to the President, foreign heads of state, or certain other persons.
3. **Worker’s Compensation.** A description that PHI may be used or disclosed as authorized by laws relating to workers’ compensation.
4. **Privacy Rule Investigation.** A description that PHI may be disclosed to the Secretary of the Department of Health and Human Services for the purpose of investigating or determining the covered entity’s compliance with the HIPAA Privacy Rule
5. OPT OUT INFORMATION

The notice must contain a statement indicating that the following uses and disclosures will be made only with authorization from the patient:

* 1. **Psychotherapy Notes.** A description of the types of uses and disclosures that require an authorization which relates to psychotherapy notes. This only applies if psychotherapy notes are being maintained by the covered entity.
  2. **Sensitive Data.** Some information, such as certain drug and alcohol information, HIV information, genetic information and mental health information is entitled to special restrictions related to its use and disclosure.
  3. **Patient’s Written Authorization.** A statement that other uses and disclosures not described in the notice will be made only with the patient’s written authorization.
  4. **Patient’s Right to Revoke.** A statement that the patient may revoke this authorization at any time in writing.
  5. **Facility Directory.** We may include certain limited information about you in the facility directory while you are a patient. This information may include your name, location in the facility, your general condition (e.g., good, fair, etc.) and your religious affiliation. Unless there is a specific written request from you to the contrary, this directory information, except for your religious affiliation, may also be released to people who ask for you by name. Your religious affiliation may be given to a member of the clergy, such as a priest or rabbi, even if they don’t ask for you by name. This information is released so your family, friends and clergy can visit you in the facility and generally know how you are doing.
  6. **Fundraising Opt-Out.** A separate statement if they contact patients to raise funds for the provider, which informs patients of this activity and that the patient has a right to opt out of receiving fundraising communications.

1. PATIENT RIGHTS

The notice must contain a statement of the patient’s rights with respect to PHI and how he or she may exercise the right to:

1. Inspect and copy PHI.
2. Amend PHI.
3. Receive an accounting of disclosures of PHI.
4. Request restrictions on certain uses and disclosures of information including a statement that the provider is not required to agree to a requested restriction except one circumstance: If a patient pays in full for a health procedure which would normally be billed to a health plan, the covered entity must agree to the request to not to share information about that procedure or item with the health plan.
5. Receive confidential communications of PHI.
6. A covered health care provider must permit patients to request and must accommodate reasonable requests by patients to receive communications of protected health information from the covered health care provider by alternative means or at alternative locations if the patient clearly states that the disclosure of all or part of that information could endanger the patient.
7. A covered entity may require the patient to make a request for a confidential communication in writing but may not require an explanation from the patient as to the basis for the request as a condition of providing communications on a confidential basis.
8. A health plan may require that a request contain a statement that disclosure of all or part of the information to which the request pertains could endanger the patient.
9. Obtain a paper copy of the notice upon request (even if the patient has agreed to receive the notice electronically). Include a statement that the agency or organization will provide a copy or a summary of the patient's health information within a certain time frame for a reasonable, cost-based fee.
10. PROVIDER DUTIES

The notice must contain:

1. Maintain the privacy of PHI, provide patients with notice of its legal duties and privacy practices, and notify patients following a breach of unsecured PHI.
2. A statement that the covered entity is required by law to maintain the privacy of PHI and to provide patients with notice of its legal duties and privacy practices with respect to PHI.
3. A statement that the covered entity is required to abide by the terms of the notice currently in effect.
4. The notice should state that the provider reserves the right to change the terms of its notice and to make the new notice provisions effective for all PHI it maintains. The statement must also explain how the provider will provide patients with a revised notice.
5. ORGANIZED HEALTH CARE ARRANGEMENT (IF APPLICABLE)

If a covered entity participates in an organized health care arrangement (OHCA) and the OHCA uses a joint notice, then the joint notice must meet the implementation specifications set forth above, except that the statements may be altered to reflect the fact that the notice covers more than one covered entity; and must:

1. Describe with reasonable specificity the covered entities, or class of entities, to which the joint notice applies;
2. Describe with reasonable specificity the service delivery sites, or classes of service delivery sites, to which the joint notice applies; and
3. If applicable, state that the covered entities participating in the organized health care arrangement will share PHI with each other, as necessary to carry out treatment, payment, or health care operations relating to the OHCA.
4. **More Stringent State Law.** If a use or disclosure for any purpose described in the Privacy Rule is prohibited or materially limited by other applicable law, the description of such use or disclosure must reflect the more stringent law.
5. **Sufficient Detail.** For each purpose described in the Privacy Rule, the description must include sufficient detail to place the patient on notice of the uses and disclosures that are permitted or required by the Privacy Rule and other applicable law.
6. **Authorization Required for Other Uses and Disclosures.** A statement that other uses and disclosures will be made only with the patient’s written authorization and that the patient may revoke such authorization.
7. [If Applicable] **Group Health Plan.** A statement that a group health plan, or a health insurance issuer or HMO with respect to a group health plan, may disclose PHI to the sponsor of the plan. To comply with GINA, health plans are required to include a statement in their NPPs that they are prohibited from using or disclosing genetic information of an patient for underwriting purposes.
8. [If Applicable] **Group Health Plan - Revisions to the Notice**. The Final Rule requires a health plan that currently posts its NPP on its website to prominently post the material change or its revised notice on its website by the effective date of the material change to the notice (i.e., the compliance date); and provide the revised notice, or information about the material change and how to obtain the revised notice, in its next annual mailing to patients then covered by the plan, such as at the beginning of the plan year or during open enrollment. If a health plan does not have a customer service website, then the health plan must provide the revised NPP, or information about the material change and how to obtain the revised notice, to patients covered by the plan within 60 days of the material revision to the notice.
9. [If Applicable] **Health Information Exchange.** Consider providing examples of the covered entity’s participation in Health Information Exchange (HIE) or Accountable Care Organization initiatives.
10. COMPLAINTS

The notice must explain that patients may file a complaint with the provider and/or the Secretary of the U.S. Department of Health and Human Services, if they believe their privacy rights have been violated. A brief description of how to file a complaint with the provider must be included. The notice also must include a statement that he patient will not be retaliated against for filing a complaint.

1. CONTACT INFORMATION

The notice must contain the name or title, and telephone number, of a person or office to contact for further information (i.e. Privacy Officer).

1. EFFECTIVE DATE

The notice must contain its effective date, which must not be earlier than the date the notice was printed or otherwise published.

1. FONT SIZE

California law requires that information produced by a hospital regarding patients’ rights be printed in 12-point font or larger [Health and Safety Code §123222.1]. The *Notice of Privacy Practices*, since it contains information about patients’ privacy rights, should thus be printed in 12-point font or larger.

1. California law has several restrictions in this area. Please see FNL SHIPM NPP Attachment A for examples. [↑](#footnote-ref-1)