



HIPAA Privacy and Security Notice of Privacy Practices

One Page Summary of Privacy Notice

Overview

This Summary of Privacy Practices summarizes how medical information about you may be used and disclosed by Menlo School's group health plan (the "Plan") or others in the administration of your claims, and certain rights that you have. For a complete, detailed description of all privacy practices, as well as your legal rights, please refer to the accompanying Notice of Privacy Practices.

Our Pledge Regarding Health Information

We are committed to protecting your protected health information. We are required by law to (1) make sure that any health information that identifies you is kept private; (2) provide you with certain rights with respect to your health information; (3) give you a notice of our legal duties and privacy practices; and (4) follow all privacy practices and procedures currently in effect.

How We May Use and Disclose Protected Health Information About You

We may use and disclose your protected health information without your permission to facilitate your medical treatment, for payment of any medical treatments, and for any other health care operation. We will disclose your health information to employees of Menlo School as necessary for plan administration functions; but those employees may not share your information for employment-related purposes. We may also use and disclose your protected health information without your permission as allowed or required by law. Otherwise, we must obtain your written authorization for any other use and disclosure of your health information. We cannot retaliate against you if you refuse to sign an authorization or revoke an authorization you had previously given.

Your Rights Regarding Your Protected Health Information

You have the right to inspect and copy your health information, to request corrections of your health information, and to obtain an accounting of certain disclosures of your health information. You also have the right to request that additional restrictions or limitations be placed on the use or disclosure of your medical information, or that communications about your medical information be made in different ways or at different locations.

How to File Complaints

If you believe your privacy rights have been violated, you have the right to file a complaint with us or with the Office for Civil Rights. We will not retaliate against you for making a complaint.



HIPAA Privacy and Security Notice of Privacy Practices

**THIS NOTICE DESCRIBES HOW YOUR HEALTH INFORMATION MAY BE USED AND DISCLOSED
AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE READ IT CAREFULLY.**

Table of Contents

Introduction	2
Contact Information	2
Effective Date	3
Protected Health Information (PHI)	3
Our Responsibilities	3
Changes to This Notice	3
HIPAA Privacy and Security Officers.....	3
How We May Use and Disclose Your PHI.....	4
Special Situations for Use and Disclosure of Your PHI.....	5
Required Disclosures.....	6
Other Disclosures	6
Security Breach	7
Your Rights	7
Complaints	9

Introduction

Menlo School sponsors the Menlo School Employee Benefits Plan (ERISA Plan 501), which includes various benefits that constitute group health plans under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), including, but not limited to: medical, dental and health care flexible spending account benefits. The Menlo School Employee Benefits Plan (the "Plan" or "We") has been established and maintained to provide benefits to our employees, their dependents and other participants. We provide this coverage through various relationships with third parties that establish networks of providers, coordinate your care, and process claims for reimbursement for the services that you receive.

This Notice describes the legal obligations of the Plan and your legal rights regarding your Protected Health Information (PHI) held by the Plan under HIPAA. Among other things, this Notice describes how your PHI may be used or disclosed to carry out treatment, for claim payment, for health care operations, or for other purposes that are permitted or required by law. It describes your rights with respect to your PHI and how you can exercise those rights. We are required to provide this Notice of Privacy Practices (the "Notice") to you pursuant to HIPAA.

Note: If you are covered by one or more fully-insured group health plans offered by Menlo School, you will receive a separate notice directly from the insurance carrier.

Contact Information

If you have any questions about this Notice or about our privacy practices, please contact the HIPAA Privacy Officer. The Privacy Officer works closely with the Security Official and is charged with the responsibility of confirming compliance and responding to all inquiries.



HIPAA Privacy and Security Notice of Privacy Practices

Carla Diez-Canseco
Menlo School
50 Valparaiso Ave
Atherton, CA 94027
Phone: (650) 330-2001

Effective Date

This Notice was initially effective July 1, 2020 pursuant to regulatory guidance as required under the HITECH Act.

Protected Health Information (PHI)

The HIPAA Privacy Rule protects only certain health information known as protected health information. This includes demographic information and health information collected from you or created or received by a health care provider, by the plan, or by Menlo School on behalf of a group health plan that relates to a past, present or future physical or mental condition. It is health information that relates to the provision of health care to you; or to the past, present or future payment for the provision of health care. Further, it is health information that could be used to identify an individual or for which there is a reasonable basis to believe that it could be used to identify an individual. PHI includes information of persons living or deceased.

Our Responsibilities

We are required by law to:

- Maintain the privacy of your protected health information and electronic protected health information;
- Provide you with certain rights with respect to your protected health information and electronic protected health information;
- Provide you with a copy of this Notice detailing our legal duties and privacy practices with respect to your protected health information and electronic protected health information;
- Follow the terms of the Notice that is currently in effect; and
- Notify you in the event of a breach of Protected Health Information.

Changes to This Notice

We reserve the right to change the terms of this Notice at any time, as allowed or required by law. We reserve the right to make any revisions or to change or make new provisions of this Notice effective for PHI that we already maintain, as well as for PHI that we receive in the future. Except as provided within this Notice, we may not disclose your protected health information without your prior authorization. If we make any material change to this Notice, we will provide you with a copy of the revised Notice of Privacy Practices by a means consistent with how other employee benefit plan information is disseminated (typically by mail, e-mail, or hand delivery).

HIPAA Privacy and Security Officers

The HIPAA Privacy Officer is an appointed person who is responsible for the development and implementation of the HIPAA Privacy policy and procedures. The HIPAA Privacy Contact Person is an appointed person who is designated to provide information and receive complaints regarding HIPAA privacy issues. These positions may change over time and may be designated as the same or different individuals. Contact information for the HIPAA Privacy Officer and HIPAA Privacy Contact Person may be found in Menlo School's HIPAA Privacy and Security Policy.

The HIPAA Security Official is an appointed person who is responsible for the development and implementation of the Plan's policies and procedures relating to security and the safeguarding of protected



HIPAA Privacy and Security Notice of Privacy Practices

health information and electronic protected health information. The HIPAA Security Official position may be held by the same individual as the Privacy Officer and/or Privacy Contact Person and may change over time. Contact information for the HIPAA Security Official may be found in Menlo School's HIPAA Privacy and Security Policy.

How We May Use and Disclose Your PHI

Under the law, we may use or disclose your PHI under certain circumstances without your permission. The following categories describe the different ways that we may use and disclose your PHI. For each category of uses and disclosures, we will explain what we may use and disclose and present some examples. Not every use or disclosure in a category will be listed. However, all of the ways we are permitted to use and disclose information will fall within one of the categories.

For Treatment: We may use or disclose your PHI to facilitate medical treatment or services by providers. We may disclose medical information about you to providers, including doctors, nurses, technicians, medical students, or other hospital personnel who are involved to take care of you. For example, we might disclose information about your prior prescriptions to a pharmacist or medical provider to determine if prior prescriptions contradict a pending prescription or is dangerous for you to use.

For Payment: We may use or disclose your PHI to determine your eligibility for Plan benefits, to facilitate payment for the treatment and services you receive from health care providers, to determine benefit responsibility under the Plan or to coordinate Plan coverage. For example, we may tell your health care provider about your medical history to determine whether a particular treatment is experimental, investigational, or medically necessary, or to determine whether the Plan will cover the treatment. We may also share your protected health information or electronic protected health information with a utilization review or pre-certification service provider. Likewise, we may share your PHI with another entity to assist with the adjudication or subrogation of health claims or to another health plan to coordinate benefit payments. We may also share your PHI, at your request, that is contained on claims submitted by medical or dental providers in an effort to verify that claims were paid correctly or to advocate for a correction in how claims were paid.

For Health Care Operations: We may use or disclose your PHI for other Plan operations. These uses and disclosures are necessary to run the Plan. For example, we may use medical information in connection with conducting quality assessment and improvement activities, underwriting, premium rating, and other activities relating to Plan coverage; submitting claims for stop-loss coverage, conducting or arranging for medical review, legal services, audit services, and fraud/abuse detection programs; business planning and development such as cost management and plan renewal management so that informed decisions can be made regarding any such prospective changes to benefit plans; and business management and general Plan administrative activities, including evaluating an employee's eligibility and administering the employee benefit plans or to providing you with information about benefits available to you under your current benefits plans. The Plan is prohibited from using or disclosing PHI that is genetic information about an individual for underwriting purposes.

To Business Associates, Subcontractors, Brokers, or Agents: We may contract with individuals or entities known as Business Associates to perform various functions on our behalf or to provide certain types of services. In order to perform these functions or to provide these services, Business Associates will receive, create, maintain, use and/or disclose your PHI, but only after they agree, in writing with us, to implement appropriate safeguards regarding your PHI. For example we may disclose your PHI to a Business Associate to administer claims or to provide support services such as utilization management, pharmacy benefit management or subrogation, but only after the Business Associate enters into a Business Associate Agreement with us. Our Business Associates are required to have each of their subcontractors or agents agree in writing to provisions that impose at least the same obligations to protect PHI as are imposed on Business Associates by the Business Associate Agreement required by HIPAA regulations.



HIPAA Privacy and Security Notice of Privacy Practices

As Required by Law: We will disclose your PHI when required to do so by federal, state or local law for law enforcement or specific government functions. For example, we may disclose your PHI when required to do so by national security laws or public health disclosure laws, or to a governmental agency or regulator with health care oversight responsibilities.

To Avert a Serious Threat to Health or Safety: We may use and disclose your PHI when necessary to prevent a serious threat to your health or safety, or the health and safety of the public or another person. Any disclosure however, would only be to someone able to help prevent the threat. For example, we may disclose your PHI in a proceeding regarding the licensure of a physician, to federal, state or local agencies engaged in disaster relief, or to private disaster assistance agencies to allow such entities to carry out their responsibilities in specific disaster situations.

To Plan Sponsors: For the purpose of administering the Plan, we may disclose PHI to certain employees of the Plan Sponsor. However, those employees will only use or disclose that information as necessary to perform plan administrative functions or as otherwise required by HIPAA, unless you have authorized further disclosures. Your PHI cannot be used for employment purposes without your specific authorization.

Special Situations for Use and Disclosure of Your PHI

In addition to the use and disclosure categories above, the following categories describe other possible ways that we may use and disclose your PHI. For each category of uses or disclosures, we will explain what we mean and present some examples. Not every use or disclosure in a category will be listed. However, all of the ways we are permitted to use and disclose information will fall within one of the categories.

Organ and Tissue Donation: If you are an organ donor, we may release your PHI to organizations that handle organ procurement or organ, eye or tissue transplantation or to an organ donation bank, as necessary to facilitate organ or tissue donation and transplantation.

Military and Veterans: If you are a member of the armed forces, we may release your PHI as required by military command authorities. We may also release PHI about foreign military personnel to the appropriate foreign military authority.

Worker's Compensation: We may release your PHI for workers' compensation or similar programs. These programs provide benefits for work related injuries or illness.

Public Health Risks: We may disclose your PHI for public health actions or when required by public health disclosure laws. These actions generally include the following:

- To prevent or control disease, injury or disability;
- To report births and deaths;
- To report child abuse or neglect;
- To report reactions to medications or problems with products;
- To notify people of recalls of products they may be using;
- To notify a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition;
- To notify state or local health authorities, as required, regarding particular communicable diseases;
- To notify the appropriate governmental authority if we believe that a patient has been the victim of abuse, neglect, or domestic violence. We will only make this disclosure if you agree in writing, or when required or authorized by law.

Health Oversight Activities: We may disclose your PHI to a health oversight agency for activities authorized by law. These oversight activities include, for example: audits, investigations, inspections and licensure. These activities are necessary for the government to monitor the health care system, government programs, and compliance with civil rights laws.



HIPAA Privacy and Security Notice of Privacy Practices

Lawsuits and Disputes: If you are involved in a lawsuit or a dispute, we may disclose your PHI in response to a court or administrative order. We may also disclose your PHI in response to a subpoena, discovery request, or other lawful process by someone else involved in the dispute, but only if efforts have been made to tell you about the request or to obtain an order protecting the information requested.

Law Enforcement: We may disclose your PHI in response to a request by a law enforcement official. For example:

- In response to a court order, subpoena, warrant, summons, or similar process;
- To identify or locate a suspect, fugitive, material witness, or missing person;
- About the victim of a crime, if under certain limited circumstances, we are unable to obtain the victim's agreement;
- About a death that we believe may be the result of criminal conduct;
- About criminal conduct, and
- In emergency circumstances to report a crime, the location of the crime or victim, or the identity, description or location of the person who committed the crime.

Coroner, Medical Examiners and Funeral Directors: We may release PHI to a coroner or medical examiner. This may be necessary, for example, to identify a deceased person or determine the cause of death. We may also release medical information about patients to funeral directors as necessary to carry out their duties.

National Security and Intelligence Activities: We may release your PHI to authorized federal officials for intelligence, counter intelligence and other national security activities authorized by law.

Inmates: If you are an inmate of a correctional institution or are under the custody of a law enforcement official, we may disclose your PHI to the correctional institution or law enforcement official if necessary (1) for the institution to provide you with health care; (2) to protect your health and safety or the health and safety of others; or (3) for the safety and security of the correctional institution.

Research: We may disclose your PHI to researchers when (1) the individual identifiers have been removed, or when an institutional review board or privacy board has reviewed the research proposal, and (2) established protocols to ensure the privacy of the requested information and approved the research.

Required Disclosures

The following is a description of disclosures of your PHI we are required to make.

Government Audits: We are required to disclose your PHI to the Secretary of the United States Department of Health and Human Services when the Secretary is investigating or determining our compliance with the HIPAA Privacy and Security rules.

Disclosures to You: Upon request, we are required to disclose to you the portion of your PHI that contains medical records, billing records, and any other records used to make decisions regarding your health care benefits. We are also required, when requested, to provide you with an accounting of most disclosures of your PHI where the disclosure was for reasons other than for payment, treatment, or health care operations, and if the PHI was not disclosed pursuant to your individual authorization.

Notification of a Breach. We are required to notify you in the event that we (or one of our Business Associates) discover a breach of your unsecured PHI, as defined by HIPAA.

Other Disclosures

Other uses and disclosures of PHI not covered by this Notice or the laws that apply to us will be made only with your written authorization.



HIPAA Privacy and Security Notice of Privacy Practices

Authorizations: Other uses or disclosures of your PHI not described above, including the use and disclosure of psychotherapy notes and the use or disclosure of PHI for fundraising or marketing purposes, will not be made without your written authorization. If you provide us with an authorization to use or disclose PHI about you, you may revoke that authorization at any time, so long as the revocation is in writing. Once we receive your written revocation, we will no longer use or disclose PHI about you for the reasons covered by your written authorization. However, such revocation will only be effective for future uses and disclosures; it will not be effective for any information that may have been used or disclosed in reliance upon the written authorization and prior to receiving your written revocation. You should understand that all revocations are prospective and we are unable to take back any disclosures we have already made under your authorization and that we are required to retain our records of care provided to you.

Personal Representatives: We will disclose your PHI to individuals authorized by you, or to an individual designated as your personal representative, attorney-in-fact, etc. so long as you provide us with written authorization and any supporting documents (i.e. power of attorney). Note: Under the HIPAA Privacy and Security rules, we do not have to disclose information to a personal representative if we have a reasonable belief that:

1. You have been, or may be, subjected to domestic violence, abuse or neglect by such person;
2. Treating such person as your personal representative could endanger you; or
3. In the exercise of our professional judgment, it is not in your best interest to treat the person as your personal representative.

Spouses and other Family Members: With only limited exceptions, we will send all mail to the employee. This includes mail relating to the employee's spouse and other family members who are covered under the Plan, and includes mail with information on the use of Plan benefits by the employee's spouse and other family members and information on the denial of any Plan benefits to the employee's spouse and other family members. If a person covered under the Plan has requested Restrictions or Confidential Communications (see below under "Your Rights"), and if we have agreed to the request, we will send mail as provided by the request for Restrictions or Confidential Communications. Such information includes, but is not limited to, Plan statements, benefit denials, and benefit debit cards and accompanying information.

Authorizations for Psychiatric Notes, Genetic Information, Marketing, and Sale: In general, and subject to specific conditions, we will not use or disclose psychiatric notes without your authorization; we will not use or disclose PHI that is genetic information for underwriting purposes; we will not sell your PHI, i.e. receive direct or indirect payment in exchange for your PHI, without your authorization; we will not use your PHI for marketing purposes without your authorization; and we will not use or disclose your PHI for fundraising purposes unless we disclose that activity in this Notice.

Security Breach

In the event of a security breach, we will comply with regulatory notification requirements. As such, if a breach occurs, we will notify affected individuals of the breach of unsecured PHI and notify the Department of Health and Human Services (as required by regulations). If more than ten individuals are affected and cannot be contacted directly, we will post a general notification of the breach on our web site and notify local print media. If more than 500 individuals are affected by the breach, we will report the breach to well-known media outlets of the breach. We are required to keep a log of all security breaches and all individuals affected by such breaches.

Your Rights

Right to Inspect and Copy: You have the right to inspect and copy certain PHI that may be used to make decisions about your health care benefits. To inspect and copy your PHI, you must submit your request in writing to the HIPAA Privacy Contact Person. If you request a copy of the information, we may charge a reasonable fee for the costs of copying, mailing or other supplies associated with your request. We may



HIPAA Privacy and Security Notice of Privacy Practices

deny your request to inspect and copy certain types of PHI in very limited circumstances, such as PHI that is collected by us in connection with, or in reasonable anticipation of any claim or legal proceeding. If you are denied access to your medical information, you may request that the denial be reviewed by submitting a written request to the HIPAA Privacy Contact Person.

Right to Amend: If you feel that the PHI we have about you is incorrect or incomplete, you may ask us to amend the information. You have the right to request an amendment for as long as the information is kept by or for the Plan. To request an amendment, your request must be made in writing and submitted to the HIPAA Privacy Contact Person. In addition, you must provide a reason that supports your request. We may deny your request for an amendment if it is not in writing or does not include a reason to support the request. In addition, we may deny your request if you ask us to amend information that:

1. Is not part of the medical information kept by or for the Plan;
2. Was not created by us, unless the person or entity that created the information is no longer available to make the amendment;
3. Is not part of the information that you would be permitted to inspect and copy; or
4. Is already accurate and complete.

If we deny your request, you have the right to file a statement of disagreement with us and any future disclosures to the disputed information will include your statement.

Right to an Accounting of Disclosures: You have the right to request an “accounting” of certain disclosures of your PHI. The accounting will not include:

1. Disclosures for purposes of treatment, payment, or health care operations;
2. Disclosures made to you;
3. Disclosures made pursuant to your authorization;
4. Disclosures made to friends or family in your presence or because of an emergency;
5. Disclosures for national security purposes; and
6. Disclosures incidental to otherwise permissible disclosures.

To request this accounting, you must submit your request in writing to the HIPAA Privacy Contact Person as provided above under Contact Information. Your request must state the time period through which you want to receive a list of disclosures. The time period may not be longer than six (6) years, or commence before the initial effective date stated in this Notice. Your request should indicate in what form you want the list (for example, paper or electronic). The first list you request within a 12-month period will be provided free of charge. For additional lists, we may charge you the costs of providing the list. We will notify you of the cost involved and you may choose to withdraw or modify your request at that time before any costs are incurred.

Right to Request Restrictions: You have the right to request a restriction on how or where your PHI may be used or disclosed for treatment, payment, or health care operations. You also have the right to request a limit on your PHI that we disclose to someone who is involved in your care or the payment for your care, like a family member or friend. For example, you could ask that we not use or disclose information about a surgery that you had. While we will consider your request, we are not required to agree to it. However, if we do agree to the request, we will honor the restriction until you revoke it or we notify you. To request a restriction, you must make your request in writing to the HIPAA Privacy Contact Person as provided above under Contact Information. In your request, you must tell us (1) what information you want to limit; (2) whether you want to limit our use, disclosure or both; and (3) to whom you want the limits to apply, for example, disclosures to your spouse. We will not agree to restrictions on PHI uses or disclosures that are legally required, or which are necessary to administer our business.

Right to Request Confidential Communications: You have the right to request that we communicate with you about medical matters in a certain way or at a certain location if you tell us that such alternate communication is necessary to protect you from endangerment. For example, you can ask that we only contact you at work or by mail. To request confidential communications, you must make your request in writing to the HIPAA Privacy Contact Person as provided above under Contact Information. We will not ask the specific reason for your request. Your request must specify how or where you wish to be contacted. We



HIPAA Privacy and Security Notice of Privacy Practices

will accommodate all reasonable requests if you clearly provide information that the disclosure of all or part of your PHI could endanger you.

Right to a Paper Copy of this Notice: You have the right to a paper copy of this Notice. You may ask us to give you a copy of this Notice at any time. Even if you have agreed to receive this Notice electronically, you are still entitled to a paper copy of this Notice. For information regarding how to obtain a paper or electronic copy of this notice, inquire with the HIPAA Privacy Contact Person as provided above under Contact Information.

Right to Notice of a Breach: You have the right to be notified in the event of any breach of electronic Protected Health Information. In the event of any breach, you will be notified at your last known address of the nature and details of such breach and of the corrective action taken.

Complaints

If you believe your privacy rights have been violated, you may file a complaint with the Plan or with the Office for Civil Rights (a division of the Department of Health and Human Services). If you have questions about how to file a complaint or wish to file a complaint with the Plan, contact the HIPAA Privacy Contact Person for details. All inquiries and correspondence regarding the complaint should be forwarded to the HIPAA Privacy Contact Person. All complaints must be submitted in writing. You should keep a copy of any notices you send to the Plan for your records.

Information on filing a complaint with the Office of Civil Rights may be found on the Department of Health and Human Service website, at <http://www.hhs.gov/ocr/contact.html>. Complaints filed with the Office of Civil Rights should be sent to the appropriate regional office. A reference list of all regions may also be found on their website. The west coast regional office contact information is as follows:

Office for Civil Rights
U.S. Department of Health & Human Services
50 United Nations Plaza - Room 322
San Francisco, CA 94102
(415) 437-8310; (415) 437-8311 (TDD)
(415) 437-8329 FAX

You will not be penalized, or in any other way retaliated against, for filing a complaint with the Plan or with the Office of Civil Rights.