University of the Pacific
Arthur A. Dugoni
School of Dentistry

Health Information Privacy Policies and Procedures

These Health Information Privacy Policies & Procedures implement our obligations to protect the privacy of individually identifiable health information that we create, receive, or maintain as healthcare providers.

We implement these Health Information Privacy Policies and Procedures as a matter of sound business practice; to protect the interests of our patients; and to fulfill our legal obligations under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), its implementing regulations at 45 CFR Parts 160 and 164 (65 Fed. Reg 82462 (Dec. 28, 2000)) ("Privacy Rules"), as amended (67 Fed. Reg. 53182 [Aug. 14, 2002]), and state law that provides greater protection or rights to patients than the Privacy Rules.

HIPAA defines our "workforce members" as including all employees, the student body, and our Business Associates. All workforce members are obligated to follow these Health Information Privacy Policies & Procedures faithfully. Failure to do so can result in disciplinary action, including termination of your employment, or dismissal from the educational program or affiliation with University of the Pacific School of Dentistry.

These Policies & Procedures address the basics of HIPAA and the Privacy Rules that apply in our dental clinics. They do not attempt to cover everything in the Privacy Rules. The Policies & Procedures sometimes refer to forms we use to help implement the policies and to the Privacy Rules themselves when added detail may be needed.

Please note that while the Privacy Rules speak in terms of "individual" rights and actions, these Policies & Procedures use the more familiar word "patient" instead; "patient" should be read broadly to include prospective patients, patients of record, former patients, their authorized representatives, and any other "individuals" contemplated in the Privacy Rules.

If you have questions or doubts about any use or disclosure of individually identifiable health information or about your other obligations under these Health Information Privacy Policies & Procedures, the Privacy Rules or other federal or state law, consult the Privacy Officer before you act.

Table of Contents

Use and Disclosure

The School of Dentistry must not use or disclose protected health information (PHI), except as these Privacy Policies and Procedures permit or require.

The School of Dentistry will disclose a patient's PHI to that patient on request.

The School of Dentistry will disclose to a patient's personal representative PHI relevant to the representative capacity. We will not disclose to a personal representative we reasonably believe may be abusive to a patient any PHI we reasonably believe may promote or further such abuse.

The School of Dentistry may use or disclose PHI in the following types of situations, provided the procedures specified in the HIPAA Privacy Rules are followed:

- For treatment, payment or operational purposes;
- For public health activities;
- To health oversight agencies;
- To coroners, medical examiners, and funeral directors;
- To employers regarding work-related illness or injury;
- To the military;
- To federal officers for lawful intelligence, counterintelligence, and national security activities;
- To correctional institutions regarding inmates;
- In response to subpoenas and other lawful judicial processes;
- To law enforcement officers;
- To report abuse, neglect, or domestic violence;
- As required by law;
- As part of research projects; and
- As authorized by state worker's compensation laws.

Incidental uses or disclosures

The School of Dentistry will take reasonable steps to limit incidental uses and disclosures of PHI made according to an otherwise permitted or required use or disclosure.

Minimum Necessary

The School of Dentistry will use, disclose and request the minimum amount of patient information that is necessary for the intended purpose of the use, disclosure or request as required by HIPAA. Workforce members are forbidden from accessing patient information that is not necessary to do their job.

The School of Dentistry will ensure our routine or recurring requests for disclosure will disclose the minimum reasonably necessary for the purpose.

All non-routine or non-recurring requests for disclosure will be reviewed to ensure only the minimum necessary PHI for the purpose is requested or disclosed.

The School of Dentistry will rely, when reasonable, on a request to disclose PHI being for the minimum necessary, if the requester is: (a) a covered entity; (b) a professional who provides professional services

to the school and represents that the information is the minimum necessary; (c) a public Officer who represents that the information requested is the minimum necessary; or (d) a researcher presenting appropriate documentation or making appropriate representations that the research satisfies the applicable requirements of the Privacy Rules. The School of Dentistry retains the discretion to make its own minimum necessary determination for disclosures to which the standard applies.

The minimum necessary requirement does not apply where the information is disclosed to, or requested by;

- Healthcare providers for treatment purposes,
- The patient, or personal representative,
- The U.S. Department of Health and Human Services

Or when;

- A patient has signed an authorization form for the use or disclosure,
- The use or disclosure is required by law or required to comply with the Privacy Rule.

Entire Record – The School of Dentistry will not use, disclose, or request an entire record, unless the entire dental record is needed to accomplish the purpose of the use, disclosure or request, or an exception to the minimum necessary standard applies.

Safeguarding of Patient Information

The School of Dentistry will have in place appropriate administrative, technical and physical safeguards to ensure the privacy of patient information is protected. The School of Dentistry will reasonably safeguard patient information from intentional or unintentional use and disclosure in violation of HIPAA. We will also reasonably safeguard patient information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure of patient information.

Oral Communications – When possible and reasonable workforce members will speak quietly when discussing a patient's condition in a waiting room or public area.

Workforce members will avoid using patient's names and discussing treatment in public areas such as hallways, elevators and bathrooms.

Workforce members will always be alert and avoid unnecessary disclosures of patient information by monitoring voice levels and being aware of unauthorized listeners. They will conduct telephone conversations away from public areas and use speaker phones only in private.

Voicemail – Unless a patient has specifically requested not to be contacted by telephone, voicemail messages and appointment reminders may be left for patients provided they contain limited information.

Fax – Fax machines will be kept in secured locations not public areas. Any faxes sent will include a cover sheet to protect

Mail – Mail will be sent to a patient's primary address unless the patient requests an alternative address. Postcards may be sent as appointment reminders as long as the patient has not objected and the postcard contains the minimum necessary amount of patient information.

Photocopiers/printers – Any photocopiers or printers that may contain patient information in their hard drives will be wiped before we dispose of them.

Destruction of paper records – Where possible all workforce members will avoid making paper copies of patient information. When disposing of any paper patient information workforce members will use the shredding bins.

Patients and visitors – All workforce members will be alert to make sure no patients or visitors have unauthorized access to patient information or areas that are off limits to the public. Visitors who may have incidental exposure to PHI will be given the Visitors HIPAA training and their signed acknowledgement of completing the training will be kept on file.

Portable and Mobile Devices – All workforce members will be aware of, and follow, all Department of Information Technology policies regarding the use of personal mobile devices.

Portable Storage Devices – Patient information may not be downloaded onto portable storage devices such as USB drives, unless the device is appropriately encrypted, or the information is being requested by the patient themselves.

Verifying Identity

The School of Dentistry will always verify the identity of any patient, and the identity and authority of any patient's personal representative. Patients who request information over the phone and whose voices are not recognized will be asked to confirm their identity using the last four digits of their phone number. PHI requested by a party other than the patient themselves through a Records Request Form will be reviewed by both the Custodian of Records and the Privacy Officer. If PHI is requested by a government or law enforcement Officer the School of Dentistry will obtain appropriate identification and evidence of authority, such as an ID card, badge or government letterhead.

Notice of Privacy Practices

The School of Dentistry will provide a notice of our privacy practices to our patients, and anyone else who requests a copy. Our Notice and how it is provided will comply with HIPAA and applicable state law. We will revise the Notice as appropriate, and will provide the revised Notice as required by HIPAA. The School of Dentistry will make a good faith effort to obtain a written acknowledgement of receipt of our Notice from our patients. We will not use or disclose patient information in a manner that is inconsistent with our Notice, HIPAA or state law.

Authorizations

The School of Dentistry will not use or disclose patient information without having the patient sign an appropriate authorization form unless the Privacy Rule permits or requires the use or disclosure.

Designated Record Set

Pursuant to the HIPAA Privacy Rule the School of Dentistry designates the following as its "Designated Record Set" subject to access and possible amendment by patients.

Medical Records;

- Treatment notes
- All images (X-rays, photographs)
- Medical History
- Patient intake information
- Treatment Plans
- Examinations, evaluations and diagnostic tests
- Consents
- Referrals
- Medical consults, referrals and other medical information from other providers
- Correspondence with patient

Billing Records;

- Enrollment information
- Eligibility information
- Billing statements
- Financial Contracts
- Insurance Claims
- Claims adjudication

Information in our Designated Record Set is contained in AxiUm and PCMS. Electronic or paper copies can be generated from either of these systems. A limited amount of information is still retained as paper charts and is also available either as a paper copy or a scanned electronic copy.

Information in our Designated Record Set from other providers can be accessed by patients only and will not be subject to amendment.

Patient Access to Records

The School of Dentistry will keep all information in its Designated Record Set and all records for at least six years from the date they were created. The School of Dentistry will also honor all patients' rights granted by the HIPAA Privacy Rule to view, obtain and amend information contained in the Designated Record Set.

The School of Dentistry will appoint a "Custodian of Records" who is responsible for the process of receiving and processing all requests related to records.

When the Custodian of Records is absent, requests will be overseen by the Group Practice Manager.

Patients have the right to look at or get copies of their health information, with limited exceptions. Patients must make the request in writing; where possible using the Records Request Form. If patients request information that we maintain electronically, they have the right to an electronic copy. We will use the format they request unless we cannot practically do so. We will charge a reasonable cost-based fee for expenses such as supplies and labor. Patients will receive access to their requested records no

later than 15 days from the date of their request. If patients prefer, we will prepare a summary or explanation of their health information for a fee.

Record Amendment Policy and Procedure

A patient, or a personal representative, has the right to request to amend information about the patient in the designated record set if they believe the information is incorrect. The request must be in writing and must give the reason for the requested amendment. If we deny the request we will put our reason for denying the request in writing. If we agree to the amendment we will add a correction to the record and tell the patient. We will not physically alter or delete existing notes in a patient's chart. If another HIPAA covered entity tells us they have amended information about a patient, we will make the same notation in our information, as appropriate.

Alternative Communications Policy and Procedure

The Dental School will accommodate reasonable requests by patients to receive communications from us by alternative means or at an alternative location.

Restricted Disclosure

The Dental School allows patients to request restricted use or disclosure of their patient information. HIPAA requires we agree to all requests not to disclose patient information about an item or service to a health plan for purposes of carrying out payment or health care operations if the information pertains solely to a health care item or service for which we have been paid in full, unless otherwise required by law. All other requests will be considered and if agreed to will be abided by until the restriction is terminated.

Accounting of Disclosures

Upon request, we will provide patients with an appropriate accounting of disclosures.

Complaints Policy

Anyone, not just a patient, has the right to complain about the School of Dentistry's HIPAA compliance, to either the School or the federal government. The School of Dentistry will document all complaints received as well as their disposition, if any. We will not retaliate against anyone who files a complaint in good faith.

Breach Policy

When the Dental School or any of our Business Associates discovers a possible breach of unsecured patient information, we will investigate and provide timely notification in compliance with HIPAA and applicable state law. Meaning, in part, we will provide notification unless we can demonstrate, through an appropriate assessment of the relevant factors, including the four required factors, that there is a low probability that the information has been compromised.

Business Associate Policy

The Dental School will manage our relationships with Business Associates in compliance with HIPAA, and will not permit a Business Associate to access patient information unless a compliant Business Associate agreement is in place.

Marketing

The School of Dentistry will not use or disclose PHI for marketing without a patient's authorization unless the marketing is in the form of a promotional gift of nominal value that we provide, or face-to-face communication between us and the patient. Only the School of Dentistry Administration may approve subsidized marketing communications.

Fundraising

The School of Dentistry will not use or disclose a patient's PHI for fundraising purposes without the patient's authorization.

Mitigation

If the School of Dentistry, or one of our Business Associates, uses or discloses patient information in violation of our privacy policies and procedures, or in violation of the privacy rule, we will mitigate, to the extent practicable, any harmful effect known to us.

Research

The School of Dentistry will utilize its institutional review board to review research proposals and establish protocols to protect the privacy of patient information. The board will ensure that when PHI is used for research purposes the requirements of the Privacy Rule are met and when necessary the appropriate authorizations are obtained.

Waivers

The School of Dentistry will not require anyone to waive their rights under the Privacy or Breach Notification Rule, including their right to complain to HHS if they believe the Dental School or another HIPAA covered entity is not complying with HIPAA, as a condition for the provision of treatment, payment or eligibility for benefits.

Training

The School of Dentistry will train all workforce members within a reasonable time after they join the School of Dentistry to comply with the HIPAA policies and procedures that affect their jobs. When there is a material change in our policies and procedures, we will retrain the workforce member whose jobs are affected by the change within a reasonable time after the change becomes effective.

Retaliation and Intimidation Policy

The Dental School and its Business Associates will not intimidate or retaliate against anyone who exercises their rights under HIPAA, participates in a HIPAA process, files a HIPAA complaint, participates in a HIPAA investigation, compliance review, proceeding or hearing, or who appropriately opposes an act that they believe is unlawful under HIPAA.

The Dental School will not, and will not permit our Business Associates to, intimidate, threaten, coerce, or discriminate against any person, nor take any retaliatory action against anyone, because he or she;

- Exercises a HIPAA right
- Participates in a process provided for by the Privacy Rule or Breach Notification Rule
- Files a complaint with the school or with the Secretary of HHS concerning the HIPAA compliance of the Dental School or a Business Associate
- Testifies, assists, or participates in a HIPAA investigation, compliance review, proceeding, or hearing by HHS
- Opposes any act or practice that HIPAA makes unlawful, as long as the person has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of patient information in violation of the Privacy Rule.

Any workforce member discovered violating this policy will be sanctioned.

Documentation Retention

The School of Dentistry will maintain all documentation as required by HIPAA. The documentation will be retained for at least six years after its creation or last effective date, whichever is later.

State Law Compliance

The School of Dentistry will comply with the privacy laws of each state that has jurisdiction over the school, or its actions involving protected health information, that provide greater protections or rights to patients than the Privacy Rules.

HHS Enforcement

The School of Dentistry will give the U.S. Department of Health and Human Services (HHS) access to our facilities, books, records, accounts, and other information sources (including individually identifiable health information without patient authorization or notice) during normal business hours (or at other times without notice if HHS presents appropriate lawful administrative or judicial process). We will cooperate with any compliance review or complaint investigation by HHS, while preserving the rights of our practice.

Review and Revise

The School of Dentistry will review and revise our HIPAA policies and procedures as necessary and appropriate to remain in compliance with HIPAA.

Changes to our Policies and Procedures

Only the HIPAA Privacy Officer in consultation with the School of Dentistry's Administration may change these Privacy Policies and Procedures.

Sanctions Policy

School of Dentistry workforce members who violate our Privacy Policies and Procedures, the Privacy Rule or other applicable federal or state privacy laws will be subject to disciplinary action, up to and including termination of employment or dismissal.

These policies and procedures apply to all members of the School of Dentistry's workforce as defined by HIPAA, which includes but is not limited to all faculty, staff and students.

Workforce members have a responsibility to report known HIPAA violations and failure to report a known violation may result in disciplinary action.

Upon being notified of, or discovering, an alleged HIPAA violation the Privacy Officer will conduct a confidential and timely investigation and involve the appropriate administrators before assigning a level of violation and disciplinary action.

Exemptions

Victim of Crime - These sanctions will not apply to a member of the workforce who is a victim of a crime and discloses PHI to a law enforcement officer provided that; the PHI disclosed is about the suspected perpetrator of the criminal act, is disclosed for identification and location purposes, and is limited to the information allowed under HIPAA.

Whistleblower – These sanctions will not apply to a member of the workforce who discloses PHI provided that;

a) The workforce member believes in good faith that the School of Dentistry is engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the School of Dentistry potentially endangers one or more patients, workers, or the public; and

b) The disclosure is to a health oversight agency, public health authority or an attorney retained for the purpose of determining legal options of the workforce member with regard to this conduct.

The following violation levels and sanctions will be used when a workforce member is found to be in noncompliance with these policies and procedures.

Level of Violation	Examples	Minimum Disciplinary / Corrective Action
Level I: Improper and/or unintentional disclosure. Failure to demonstrate appropriate care and safeguards in handling PHI.	- Loss of unencrypted device containing PHI - Improper disposal of PHI - Discussing PHI in a non-secure area (elevator, cafeteria etc.) - Sending email containing PHI to wrong recipient - Leaving a computer with PHI logged on and unsecured - Leaving PHI in an unsecured location - Failing to report a possibly compromised password (replying to a spam email and providing password etc.) - Failing to cooperate with the Privacy Officer	- Oral warning or letter of disciplinary reprimand from most immediate supervisor
Level II: Intentional Access, Use or Disclosure without authorization	- Accessing PHI unnecessarily - Failure to verify the identity of an individual leading to inappropriate disclosure of PHI - Failure to comply with a corrective action or recommendation - A second Level I violation, not necessarily of the same kind - Assisting someone to gain unauthorized access to PHI (sharing your password etc.)	- Letter of disciplinary reprimand from Chair or Associate Dean of Clinical Affairs - Possible report to Ethics Committee - If reported, Chair or ADCA will initiate a disciplinary action plan based on recommendation from Ethics Committee.
Level III: Intentional Abuse of PHI	- Releasing or using PHI for personal gain or to cause malicious harm - Assisting someone to gain unauthorized access to PHI for their personal gain or with the intent to cause harm - Tampering or unauthorized destruction of PHI	- Written notification of suspension by ADCA with copy to Dean - Incident reported to Ethics Committee - Formal disciplinary action up to and including dismissal - Reported to any appropriate licensing or law enforcement agencies

Directory of Personnel

Current Privacy Officer:	Lindsey Green (415) 351 7124 lgreen@pacific.edu
Previous Privacy Officers:	Debbie Keatley (415) 351 7141 dkeatley@pacific.edu Eve Cuny (415) 929 6610 ecuny@pacific.edu
Current Security Officer:	Raybel Ramos (415) 929 6517 rramos@pacific.edu
Custodian of Records:	Debbie Keatley (As above)