## Important Notice

**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.**

- Effective Date: May 18, 2026
- This Notice replaces the prior Bastyr University Clinic San Diego Notice of Privacy Practices (April 28, 2016) and reflects current federal law, California state law, and current best practice for online and digital communications.

## Who Follows This Notice

This joint Notice describes the privacy practices of Bastyr University Clinic San Diego, located at (see bastyrclinics.org/san-diego for the current clinic address) together with:

- Every health-care professional authorized to enter information into your medical record at the Clinic, including employed and contracted clinical faculty, supervising providers, residents, student clinicians, and visiting professionals operating under our supervision.
- Bastyr University departments and personnel that comprise Bastyr's health-care component, including the Clinic, Bastyr's research department conducting clinical research, and select external clinic sites affiliated with Bastyr.
- Business Associates that perform functions on our behalf and that have signed a Business Associate Agreement, such as our electronic health record vendor, billing services, secure messaging vendors, shredding and records-destruction vendors, and our IT and information security vendors.

The Clinic and its independent clinical providers operate under an organized health-care arrangement under HIPAA so that information needed to coordinate your care can be shared with other providers involved in your treatment. Independent providers may have separate privacy practices when they deliver care at their own private offices.

## Our Responsibilities

Federal and state laws protect the privacy of the health information we create and obtain in providing care to you. We are required by law to:

- Maintain the privacy and security of your protected health information ('PHI').
- Give you this Notice of our legal duties and privacy practices.
- Follow the terms of the Notice that is currently in effect.
- Notify you in the event of a breach affecting your unsecured PHI.
- Comply with applicable state laws when they offer you greater privacy protection than HIPAA.

# How We Use and Disclose Your Health Information

## For Treatment

We use information about you to provide and coordinate your care. For example, your student clinician and supervising faculty review your record together to plan your treatment, order labs, prescribe natural or pharmaceutical therapies, and refer you to specialists when needed. We may share your record with referral providers — hospitals, specialists, imaging centers, pharmacies — to deliver coordinated care.

## For Payment

We use and share your information to bill you, your health plan, or another third-party payer; to obtain prior authorization; to determine eligibility and benefits; and to collect payment. We will not disclose your health information to a third-party payer for purposes other than payment without your authorization, except as permitted or required by law.

## For Health Care Operations

We use and share your information to run the Clinic — quality assessment and improvement, faculty and student-clinician education, accreditation and licensure, credentialing, business planning, and fraud-and-abuse and compliance programs. As a teaching clinic, we use de-identified or limited information in case discussions for educational purposes.

## For Appointment Reminders and Care Coordination

We may contact you with appointment reminders, lab and test results, prescription refill information, follow-up instructions, and other communications relating to your care. See the Text-Messaging Communications section below for specific information about SMS and digital communications.

## For Health Information Exchange

Our electronic health record system participates in OCHIN through 2026 and is transitioning to Athena Health. Both systems enable secure, HIPAA-compliant exchange of your information with other treating providers and authorized exchanges only when necessary for your treatment, payment, or our health-care operations. A current list of OCHIN participants is at ochin.org. If you do not wish to participate in this collaboration, please tell your supervising faculty member; we may not be able to serve you and can help you find another provider.

## Communication with Family and Friends

We may share information about you with a family member, friend, or other person you identify as involved in your care or in paying for your care. We will obtain your informal permission by asking you, or by giving you a meaningful opportunity to object, in advance of any such disclosure.

## Other Permitted Uses (Without Your Written Authorization)

- Public health activities — disease reporting, immunization information, FDA-reportable events.

- Victims of abuse, neglect, or domestic violence — per applicable law.
- Health oversight activities — audits, investigations, inspections, and licensure of clinicians.
- Judicial and administrative proceedings — in response to a court or qualifying administrative order, subpoena, or discovery request.
- Law enforcement — in narrowly defined circumstances permitted by 45 CFR §164.512(f), including the limited additional state-law protections described in the State Law Addendum below.
- Coroners, medical examiners, and funeral directors — to identify a deceased person or determine cause of death.
- Organ and tissue donation — when authorized.
- Research — only with appropriate Institutional Review Board (IRB) authorization or waiver, or with your specific written authorization when required.
- Serious threat to health or safety — to prevent or lessen a serious and imminent threat.
- Specialized government functions — military and veterans affairs, national security, and certain federal officials, as authorized by law.
- Workers' compensation — as permitted or required.
- Inmates — to a correctional institution or law-enforcement official as necessary for health and safety.

## Uses and Disclosures That Require Your Written Authorization

We will obtain your written authorization before we use or share your PHI for:

- Marketing communications (other than face-to-face communication or a promotional gift of nominal value).
- Sale of PHI — we do NOT sell your PHI.
- Most uses and disclosures of psychotherapy notes.
- Other uses and disclosures not described in this Notice.

You may revoke a written authorization at any time, in writing, except to the extent that we have already acted in reliance on it.

## Your Health Information Rights

1. RIGHT TO THIS NOTICE — you may request a paper copy of this Notice at any time, even if you previously agreed to receive it electronically.
2. RIGHT TO INSPECT AND COPY — you may inspect and receive an electronic or paper copy of your medical and billing records, in the form and format you request when readily producible. We will respond within the timeframe required by federal and state law. The medical record itself remains the property of the Clinic, but the information in it belongs to you. We may charge a reasonable, cost-based fee. We may deny your request in limited circumstances; you may request review of any denial.
3. RIGHT TO ELECTRONIC ACCESS (21st Century Cures Act) — you may access your electronic health record through the patient portal at no charge. Information blocking is not permitted; if you cannot get the information you have requested, please contact our Privacy Officer.
4. RIGHT TO REQUEST AMENDMENT — if you believe information in your record is inaccurate or incomplete, you may request an amendment in writing. We may deny the request in limited circumstances and will provide a written explanation; you may submit a statement of disagreement that we will include with any release of your records.
5. RIGHT TO AN ACCOUNTING OF DISCLOSURES — you may request a list of disclosures we have made of your PHI for purposes other than treatment, payment, or operations, for up to six (6) years before the date of your request. The first list within a 12-month period is free; we may charge a cost-based fee for additional lists with advance notice.
6. RIGHT TO REQUEST RESTRICTIONS — you may request that we restrict certain uses or disclosures. We are not required to agree, except that we will accept your request to restrict disclosure to a health plan when you have paid in full out of pocket for the related service (HITECH §13405(a)).
7. RIGHT TO REQUEST CONFIDENTIAL COMMUNICATIONS — you may ask us to contact you in a specific way (for example, by mobile phone only) or at a specific location. We will accommodate reasonable requests.
8. RIGHT TO REVOKE AUTHORIZATION — you may revoke an authorization at any time in writing, except as already acted upon.
9. RIGHT TO BREACH NOTIFICATION — we will notify you if a breach of your unsecured PHI occurs.
10. RIGHT TO FILE A COMPLAINT — without fear of retaliation. See the Complaints section below.

# California Law Addendum

California law provides additional protections that supplement HIPAA. Where California law is more protective than HIPAA, we follow California law.

## Confidentiality of Medical Information Act (CMIA — California Civil Code §56 et seq.)

- California provides broader definitions of 'medical information' and 'provider of health care' than HIPAA, with additional disclosure restrictions and statutory penalties of $1,000 to $250,000 for improper disclosure.
- Under AB 254 (effective January 1, 2024), 'medical information' includes 'reproductive or sexual health application information' — meaning information about reproductive health, menstrual cycle, fertility, pregnancy, pregnancy outcome, plans to conceive, or sexual activity collected by a reproductive or sexual health digital service. We treat this category as CMIA-protected medical information.
- Patient access to records: we will permit inspection within 5 working days of a written request and provide a copy within 15 days; reasonable cost-based fees apply.

## AB 352 — Segmentation of Sensitive Services

- By July 1, 2024, businesses electronically storing medical information on 'sensitive services' (gender-affirming care, abortion and abortion-related services, contraception) were required to develop capabilities to limit access to, prevent disclosure of, and segregate that information.
- Beginning January 31, 2026, we do not knowingly disclose or transmit medical information through our electronic health record or any health-information exchange that would identify an individual seeking, obtaining, providing, supporting, or aiding lawful abortion or gender-affirming care to a person or entity outside California, unless specifically authorized by you in writing or as otherwise permitted by California law.

## California Consumer Privacy Act / California Privacy Rights Act (CCPA/CPRA)

PHI we collect and maintain as a HIPAA-covered health-care provider is generally exempt from CCPA/CPRA. For information we collect that falls outside that exemption (for example, certain information collected through our public website or marketing channels), the following rights apply for California residents:

- RIGHT TO KNOW — what categories of personal information we collect, the purposes, and the categories of third parties with whom we share.
- RIGHT TO DELETE — your personal information, subject to legal record-retention exceptions.
- RIGHT TO CORRECT — inaccurate personal information.
- RIGHT TO LIMIT USE OF SENSITIVE PERSONAL INFORMATION.
- RIGHT TO OPT OUT — of the sale of personal information and of sharing for cross-context behavioral advertising. We do not sell your personal information.
- RIGHT TO NON-DISCRIMINATION — for exercising these rights.

- RIGHT TO DESIGNATE AN AUTHORIZED AGENT — to exercise these rights on your behalf.
- Verification: we will verify your identity using reasonable methods before fulfilling a request. We will respond within 45 days, with one 45-day extension permitted when reasonably necessary.

## Reproductive & Gender-Affirming Health Care

- Consistent with California law, we do not voluntarily disclose information about lawful reproductive or gender-affirming care for use in any out-of-state criminal, civil, or administrative investigation or proceeding to identify, prosecute, or harm a patient, provider, or anyone who assists.
- We apply HIPAA's Minimum Necessary standard and the AB 352 segmentation requirements to all sensitive-services information.
- Note: a federal court vacated the substantive provisions of the 2024 HIPAA Privacy Rule to Support Reproductive Health Care Privacy in June 2025 (Purl v. HHS); the California protections described above continue regardless of that ruling.

## Mental Health, Substance Use & Other Specialized Records

- Mental-health records receive additional protection under the Lanterman-Petris-Short Act (Welfare & Institutions Code §5328 et seq.).
- Substance-use disorder records, where applicable, receive additional federal protection under 42 CFR Part 2.
- Genetic information receives additional protection under the California Genetic Information Privacy Act.
- Information about HIV and AIDS receives additional protection under California Health & Safety Code §120975 et seq.

## Breach Notification

- California requires CMIA-covered breach notification to affected individuals and, when more than 500 California residents are affected in a single breach, to the California Attorney General as required by Civil Code §1798.29 and §1798.82.
- We will notify affected individuals within the timeframes required by HIPAA (no later than 60 calendar days after discovery) and California law (within 15 business days for CMIA breaches that meet the threshold).

# Text-Messaging (SMS / RCS) Communications

We may use SMS and RCS text messaging to communicate with patients about appointment reminders, billing notifications, lab-result availability, and care coordination. The following terms govern our text-messaging program (consistent with current CTIA carrier guidance).

## How we collect and use mobile numbers

- We collect mobile phone numbers to communicate with patients via SMS and/or RCS for purposes such as appointment reminders, billing notifications, lab-result availability, and care coordination.
- Your privacy is a priority. Your mobile number will not be sold or shared with third parties or affiliates for marketing or promotional purposes. We will not use your number for unrelated marketing without your express written consent.

## Texting terms

- Bastyr University Clinic San Diego uses text messaging to communicate with patients for purposes such as appointment reminders, billing notifications, and care coordination. You are not required to opt in as a condition of receiving care. Participation is voluntary. However, opting out may prevent us from sending you timely updates regarding your care.
- Message frequency may vary.
- Message and data rates may apply.
- Carriers are not liable for delayed or undelivered messages.
- Text messages sent via SMS and RCS channels are not fully secure and may not be HIPAA-compliant; however, we take reasonable precautions to safeguard your privacy by restricting the content of these messages to non-sensitive notifications. Any messages containing detailed Protected Health Information (PHI) will be sent via a separate, secure messaging channel (our patient portal).
- You may opt out of receiving text messages at any time by replying STOP. You will receive a final confirmation text to verify you have opted out; no further messages will be sent. If you would like to rejoin, you can authorize us to restart by texting START.
- For help, reply HELP or contact us at the Clinic's main number listed at bastyrclinics.org/san-diego and/or the patient-services email listed at bastyrclinics.org/san-diego.

## Website, Cookies & Tracking Technologies

Our public website (bastyrclinics.org) uses cookies and other tracking technologies for basic site function, accessibility, and analytics. We have reviewed our use of online tracking technologies in light of HHS Office for Civil Rights guidance and have removed third-party tracking pixels and similar technologies from any page authenticated to your protected health information (such as the patient portal).

- On unauthenticated pages, we may use first-party and limited third-party analytics to understand site traffic and improve usability.
- We do not use tracking technologies on the patient portal.
- We do not sell information collected through our website.

You may control cookies through your browser settings. Some site features may not function without cookies.

## Telehealth & Patient Portal

- When you participate in a telehealth visit, the same federal and state privacy protections apply as in a face-to-face visit. Our telehealth platform is HIPAA-compliant and a Business Associate Agreement is in place.
- Patient-portal messages and document exchanges are encrypted in transit and at rest.
- You may communicate with your care team through the patient portal. Avoid using personal email for sharing health information; if you choose to, you accept the inherent security risk of unencrypted email.

## Marketing, Fundraising & Educational Communications

- TREATMENT ALTERNATIVES & HEALTH BENEFITS — we may tell you about treatment options, health-related benefits, services, and educational classes that may be of interest to you.
- FUNDRAISING — we may contact you as part of a Bastyr fundraising effort. We will provide a clear way to opt out of receiving future fundraising requests. We will not use your medical-record content for fundraising; demographic and limited information may be used per HIPAA.
- MARKETING — we do not use your PHI for marketing communications without your written authorization, except for face-to-face communication or a promotional gift of nominal value.

## Breach Notification

If a breach of your unsecured PHI occurs, we will notify you in writing without unreasonable delay and no later than 60 calendar days after discovery. Notification will include a description of what happened, the information involved, the steps we are taking, and what you can do to protect yourself.

## Changes to This Notice

We reserve the right to change this Notice at any time. Any revised Notice will be effective for the health information we already have about you as well as any information we receive in the future. The current version is posted in the Clinic and on our website, and will be made available to you on request.

## Complaints & Contact

**HOW TO CONTACT US OR FILE A COMPLAINT**

- Privacy Officer: BUSD Privacy Officer — see bastyrclinics.org/san-diego for current contact
- Address: Bastyr University Clinic San Diego 4110 Sorrento Valley Blvd, San Diego, California 92121
- U.S. Department of Health and Human Services, Office for Civil Rights — 200 Independence Avenue SW, Washington DC 20201 · 1-877-696-6775 · www.hhs.gov/ocr
- The quality of your care will not be jeopardized, nor will you be penalized for filing a complaint.

## California-Specific Complaint Avenues

- California Office of the Attorney General — Privacy Enforcement and Protection Unit (oag.ca.gov/privacy).
- California Department of Public Health — Licensing & Certification (for clinic licensure).
- California Civil Rights Department — for discrimination complaints related to access to care.

## Effective Date

This Notice is effective May 18, 2026 and replaces all prior versions of the Bastyr University Clinic San Diego Notice of Privacy Practices, including the April 28, 2016 joint BCNH/BUSD Notice.