Privacy Policy

Bioprium — [LEGAL ENTITY NAME]

Table of Contents

Effective Date	[EFFECTIVE DATE]
Version	1.0
Last Updated	[DATE]
Document Owner	[NAME, TITLE]
Status	Draft — pending review by qualified counsel

Applies to bioprium.com, the Bioprium web application, the Bioprium command-line and container distributions, and all associated services (collectively, the **"Service"**).

> ***DRAFT — FOR COUNSEL REVIEW ONLY.*** *This document was prepared with AI assistance and has **not** been reviewed by a licensed attorney. It is not legal advice. It must be reviewed by counsel qualified in US health privacy law (HIPAA/HITECH), state genetic privacy law, and US state consumer privacy law before publication. Every bracketed placeholder must be resolved, and every factual claim about security controls, subprocessors, retention periods, and website tracking must be independently verified as true before this document is published.*

HOW TO READ THIS POLICY

This document is longer than most privacy policies because Bioprium processes an unusually sensitive category of information: human genomic sequence data and the clinical inferences derived from it. We would rather be exhaustive than leave you guessing.

Three audiences, three starting points:

If you are a **hospital, health system, laboratory, or research institution** evaluating Bioprium, start with Section 4 (our role), Section 6 (consent obligations), Section 14 (your rights and controls), and Section 24 (disclaimers and liability).

If you are a **patient** whose genomic data may be processed through Bioprium by your care provider, start with Section 12 (how we handle genetic information), Section 18 (your rights and how to exercise them), and Section 19 (state-specific disclosures).

If you are an **individual creating an account or purchasing a subscription**, start with Section 8 (what we collect about you), Section 18 (your rights), and Section 26 (how we handle changes to this policy).

The single most important thing on this page: Bioprium does not obtain consent from patients. If your genomic data reaches Bioprium, it reaches us because a hospital or other covered healthcare entity sent it to us, and that entity is responsible for having obtained your consent or authorization first. See Section 6.

---

1. CURRENT SERVICE STATUS — READ BEFORE ANYTHING ELSE

Bioprium is a pre-commercial company. The Service is under active development. This section states plainly what is operational today and what is not, so that no reader mistakes a forward-looking commitment for a present capability.

1.1 What the Service does today

As of the Effective Date, the Bioprium software:

- Operates on **publicly available reference and benchmark datasets only** — including the 1000 Genomes Project, the Human Pangenome Reference Consortium (HPRC), the IPD-IMGT/HLA database, GRCh38 reference assemblies, and STRchive.
- Runs **locally or in a container on infrastructure controlled by the operator of the software**. It does not upload genomic files to Bioprium-operated servers.
- Contains **no user authentication, no user accounts, and no multi-tenant data separation**, because it does not yet store data belonging to more than one party.
- Is governed by an internal engineering rule ("Rule 6") that prohibits protected health information from entering the codebase, and prohibits any code path that would create a HIPAA obligation, until a formal architecture and security review has been completed and a Business Associate Agreement is in place.

1.2 What this policy governs

This policy governs **both**:

(a) The Service as it exists today — principally the Bioprium website, any evaluation or demonstration environment, sales and marketing communications, and the account-registration and subscription flows this policy gates.

(b) The hosted, account-based, PHI-processing Service that Bioprium is building toward ("the **Production Service**"). Sections concerning the receipt, storage, and processing of patient genomic data describe the Production Service. **Those sections take effect for a given Hospital only upon execution of a Business Associate Agreement and a Master Services Agreement between Bioprium and that Hospital.**

1.3 No certifications are claimed

Bioprium **does not currently hold** SOC 2 Type I or Type II attestation, HITRUST CSF certification, ISO/IEC 27001 certification, or any comparable third-party security certification. Where this policy describes security controls, those are descriptions of practices and of contractual commitments — **not** representations that any control has been audited or certified by an independent third party. Any certification Bioprium obtains in future will be listed at [TRUST PAGE URL] and identified by auditor, scope, and report date.

We state this affirmatively because a privacy policy that implies certifications a company does not hold is itself an unfair or deceptive practice under Section 5 of the FTC Act, and because hospital security reviewers will discover the absence regardless.

1.4 No patient data should be sent to us today

Until a Business Associate Agreement is executed, do not transmit protected health information, identifiable genomic data, or any patient-derived file to Bioprium through any channel — not by email, not by upload, not by shared drive, not by support ticket. If you do so, we will treat it as an inadvertent disclosure: we will not process it, we will notify the sending organization, and we will securely destroy it. See Section 21.4.

---

2. WHO WE ARE

[LEGAL ENTITY NAME], doing business as **Bioprium**, a **[STATE] [ENTITY TYPE — e.g., corporation / limited liability company]**.

Our registered address is [STREET, CITY, STATE, ZIP].

General enquiries: [GENERAL EMAIL] Privacy questions and rights requests: privacy@[DOMAIN] Security and vulnerability disclosure: security@[DOMAIN] Data Protection Officer / Privacy Officer: [NAME OR “not appointed; inquiries to privacy@”] HIPAA Privacy Official: [NAME AND TITLE] HIPAA Security Official: [NAME AND TITLE]

45 C.F.R. § 164.308(a)(2) requires a Business Associate to designate a **Security Official**. The Privacy Official requirement at § 164.530(a) is addressed to covered entities; Bioprium designates one as a matter of practice and contract rather than regulatory obligation. Both are named roles held by identified individuals, not shared inboxes.

---

3. DEFINITIONS

Terms used throughout this policy have the following meanings. Where a term is also defined by statute, the statutory definition controls for purposes of that statute.

“Aggregate Data” — statistical or summary information derived from multiple sources that does not identify, and cannot reasonably be used to identify, any individual, Hospital, or patient.

“Business Associate” — has the meaning given at 45 C.F.R. § 160.103. Bioprium acts as a Business Associate of a Hospital when it creates, receives, maintains, or transmits PHI on that Hospital’s behalf.

“Consumer Health Data” — has the meaning given under the Washington My Health My Data Act (RCW 19.373), the Nevada Consumer Health Data Privacy Law (SB 370), and comparable state statutes: personal information linked or reasonably linkable to a consumer that identifies past, present, or future physical or mental health status. This category is broader than PHI and, importantly, **can include information collected through our website that is not PHI**.

“Covered Entity” — has the meaning given at 45 C.F.R. § 160.103.

“De-identified Data” — Hospital Data from which identifiers have been removed in accordance with 45 C.F.R. § 164.514(b), by either the Expert Determination method (§ 164.514(b)(1)) or the Safe Harbor method (§ 164.514(b)(2)), together with the additional genomic-specific measures described in Section 15.3.

“Derived Data” — any output, inference, score, classification, annotation, guide sequence, dossier, report, log, provenance record, digest, or intermediate artifact produced by the Service from Hospital Data. Derived Data includes, without limitation: HLA allele calls, CAG repeat counts and band classifications, off-target site catalogs, on-target degradation assessments, contamination estimates, ancestry or superpopulation inferences, eligibility determinations, quality-control metrics, and rendered design dossiers.

“Genetic Information” — has the meaning given under the Genetic Information Nondiscrimination Act of 2008 (Pub. L. 110-233) at 42 U.S.C. § 2000ff(4) and 45 C.F.R. § 160.103, and under applicable state genetic privacy statutes. It includes information about an individual’s genetic tests, the genetic tests of that individual’s family members, and the manifestation of a disease or disorder in family members.

“Hospital” — any hospital, health system, academic medical center, clinical laboratory, research institution, biobank, physician practice, contract research organization, or other organization that establishes an account with

Bioprium and submits data to the Service. Used throughout as shorthand for "Customer," including customers that are not literally hospitals.

"Hospital Data" — all data a Hospital or its authorized users submit to, or cause to be submitted to, the Service, including genomic sequence files, variant calls, clinical annotations, sample metadata, and any PHI contained therein.

"PHI" — Protected Health Information as defined at 45 C.F.R. § 160.103.

"Service" — as defined in the header.

"Subprocessor" — a third party engaged by Bioprium that processes Hospital Data on Bioprium's behalf.

"you" — depending on context, the Hospital, an individual user of the Service, a website visitor, or a patient whose data is processed. Where a distinction matters, this policy says which.

---

4. OUR ROLE AND THE TWO DATA TIERS

Bioprium's privacy obligations differ fundamentally depending on which of two categories a given piece of information falls into. Conflating them is the most common source of confusion in health-technology privacy policies, so we separate them explicitly.

4.1 Tier One — Hospital Data (we are a Business Associate / processor)

When a Hospital submits patient genomic data to the Production Service, Bioprium acts as:

- a **Business Associate** under HIPAA, processing PHI on the Hospital's behalf and subject to a Business Associate Agreement;
- a **"service provider"** under the California Consumer Privacy Act as amended by the CPRA (Cal. Civ. Code § 1798.140(ag));
- a **"processor"** under the Virginia CDPA, Colorado CPA, Connecticut CTDPA, Texas TDPSA, Utah UCPA, Oregon, Montana, Delaware, Iowa, Nebraska, New Hampshire, New Jersey, Tennessee, Minnesota, Maryland, Indiana, Kentucky, Rhode Island, Florida, and comparable state comprehensive privacy statutes; and
- a **"processor"** under the EU GDPR and UK GDPR, where applicable.

In this tier, the Hospital is the controller and we are not. We process Hospital Data only on documented instructions from the Hospital, only for the purposes described in Section 10, and only as permitted by the applicable Business Associate Agreement. We do not decide the purposes or means of processing Hospital Data beyond what is necessary to operate the Service.

We do not have a direct relationship with patients. We do not obtain patient consent, we do not provide notices of privacy practices to patients, and we generally cannot respond directly to a patient's request about their own data. Those are the Hospital's obligations. See Section 18.

4.2 Tier Two — Account, Website, and Business Data (we are a controller)

When you visit our website, request a demonstration, correspond with us, create an account, or purchase a subscription, Bioprium acts as a **controller** (or "business" under the CCPA) with respect to that information. We decide why and how it is processed. This tier is governed by Sections 8, 17, 18, and 19.

Important: Tier Two data is not automatically outside health-privacy law. **Washington's My Health My Data Act contains data-level exemptions only — it does not exempt an entity merely because that entity is a Business Associate for other data.** Website analytics, marketing interactions, and inquiry forms that reveal a health condition or an interest in a specific disease can constitute regulated Consumer Health Data even though they are not PHI. We treat them accordingly. See Section 19.3.

4.3 What we are not

Bioprium is **not** a Covered Entity. We are not a healthcare provider, health plan, or healthcare clearinghouse. We do not practice medicine, do not provide genetic counseling, do not issue clinical diagnoses, and do not operate a clinical laboratory. Bioprium is not CLIA-certified and its outputs are not clinical laboratory results. See Section 23.

---

5. WHAT DATA WE COLLECT — HOSPITAL DATA

This section describes the categories of data the Production Service is designed to receive from Hospitals. It is written against the actual architecture of the Bioprium software rather than in generalities, because a Hospital's security reviewer will ask for exactly this level of specificity.

5.1 Genomic sequence data

The Service accepts, and refuses, specific input types:

What we accept. A whole-genome BAM is accepted and sliced on receipt to the analysis window plus the relevant alternate contigs. A whole-genome CRAM is accepted on the same basis, provided the Hospital supplies the reference explicitly — we never infer it. A pre-sliced BAM is used as supplied. A pre-sliced CRAM is accepted and converted to BAM. VCF variant calls are accepted only through the dedicated variant input path. Long-read alignments for repeat-expansion analysis are accepted.

What we refuse. FASTQ and other unaligned reads are refused; alignment must happen upstream, in the Hospital's own environment. SAM files, compressed or not, are refused. Truncated files, files with missing indexes, files whose reference does not match, and files aligned against the wrong reference build are all refused, with an error identifying the specific defect.

These validations apply to the short-read immunogenetics ingestion path. The long-read repeat-expansion path currently performs identifier validation only and passes the supplied alignment directly to the repeat caller. Extending the full validation and quality-control layer to that path is a condition precedent to accepting patient data through it. See Section 1.

Data minimization is enforced architecturally, not just by policy. Where the analysis targets a specific genomic locus, the Service slices the relevant genomic window on receipt and processes only that window. For the immunogenetics track, this is a region of chromosome 6 together with the alternate haplotype contigs on which an

aligner may have placed reads — **measured at approximately 115 MB against a 30× whole-genome CRAM of roughly 16 GB**, a reduction of more than two orders of magnitude.

Hospitals are strongly encouraged to slice before transmission so that whole-genome data never leaves the Hospital's environment at all. Bioprium publishes the slicing procedure at [DOCS URL] and provides tooling to perform it locally.

Where a Hospital transmits a whole genome, Bioprium produces and retains the slice, and deletes the source file on the schedule in Section 20.2. The ingestion record retains the source file's SHA-256 digest and its original filename for provenance; both are removed on redaction under Section 20.3.

5.2 Sample and clinical metadata

- Sample identifiers (which should be pseudonymous — see Section 5.6)
- Reference genome build and assembly identity
- Sequencing platform, instrument, and chemistry, where supplied
- Target gene, locus, or indication for the analysis
- A population or ancestry label, **where the Hospital chooses to supply one**. Bioprium does not infer ancestry. Any such label is a value the Hospital provides and Bioprium stores and groups by; it is never computed from sequence.
- Any clinical annotation the Hospital elects to supply

5.3 Derived Data — the outputs

The Service generates, stores, and returns:

- **HLA allele calls** at defined field resolution, together with caller agreement status and ambiguity sets
- **Repeat-expansion measurements**, including CAG repeat counts at the HTT locus and their classification into penetrance bands (normal / intermediate / reduced penetrance / fully penetrant)
- **Guide RNA candidates**, including protospacer sequences, PAM sites, strand, and genomic coordinates
- **Allele-selectivity scores** for candidate guides
- **Off-target site catalogs**, including sites present in a patient's personal genome that are absent from the reference genome ("patient-private" sites) and reference sites abolished in the patient
- **On-target degradation assessments**
- **Specificity scores** computed against reference and personal genomes
- **Contamination estimates**, where a suitable marker panel is available for the analysis interval. Where it is not, the Service reports the value as **not estimated** rather than as zero.
- **Quality-control metrics**, including coverage depth over the analysis interval
- **Eligibility determinations** for a given therapeutic modality
- **Phasing and haplotype assignments**
- **Rendered design dossiers** aggregating the above, with a mandatory limitations section
- **Provenance records** (see 5.4)

Derived Data is PHI. An HLA genotype, a CAG repeat count, or a catalog of patient-private off-target sites is individually identifying genomic information and is not made less sensitive by being an output rather than an input. We treat all Derived Data with the same protections as the sequence data it came from.

5.4 Provenance and audit records

Every number the Service emits carries a provenance record. These records include:

- The producing tool and its exact version
- The reference genome build and the SHA-256 digest of the reference FASTA, where a reference was consulted
- The allele registry or repeat catalog version, where one was used
- **SHA-256 digests of every input file**
- A digest of the configuration in force
- The software commit identifier, flagged if the working tree was not clean
- Run identifier and timestamp
- Structured event logs, one JSON record per line, for the run

Where a given analysis does not consult a reference or a registry, the corresponding field records that fact explicitly rather than being left blank or defaulted — the Service does not permit a provenance record to render with an unexplained gap.

A note on hashes. A SHA-256 digest of a genomic file is not anonymous. Given a candidate file, anyone can confirm a match. Digests are therefore treated as PHI, stored with the same protections, and deleted on the same schedule as the files they describe.

Provenance records exist for a reason that matters to you as well as to us: software whose basis a qualified professional can independently review and reject is more likely to be treated as Clinical Decision Support rather than as a regulated medical device. Traceability is a safety and regulatory property, not documentation hygiene.

5.5 Where data is written

For transparency, and because a Hospital's security reviewer will ask, these are the persistent artifacts a run produces. Each is subject to the retention schedule in Section 20 and to Hospital deletion instructions:

- The sliced analysis interval and its index
- An ingestion record recording the source filename, its digest, and the sample identifier
- A structured event log for the run, keyed by run identifier, containing sample identifiers and file paths
- The rendered dossier and its structured representation
- A record in the design registry, keyed by allele or target, whose payload includes the sample identifier, the input digest, quality-control results, the genotype, and the selected guide with its off-target set
- Where a validation construct is generated, a sequence file **whose filename contains the sample identifier**
- Cached reference artifacts, which contain no patient data

Two properties of these artifacts that Hospitals should know about. First, the design registry is append-only by design — immutability is the property that makes design provenance trustworthy, and it is deliberately not deletable in the current architecture. See Section 20.3, which explains how this is reconciled with deletion obligations and what must change before the Production Service accepts PHI. Second, event logging is currently written to fail silently rather than to interrupt a run; for the Production Service, audit logging of PHI access will be made a blocking operation, because an audit log that can be lost without a signal is not an audit log.

5.6 What we ask Hospitals NOT to send

The Service does not require, and Hospitals should not transmit:

- Patient names, medical record numbers, dates of birth, addresses, telephone numbers, email addresses, Social Security numbers, insurance identifiers, or any of the eighteen identifier categories enumerated at 45 C.F.R. § 164.514(b)(2)
- Free-text clinical narrative
- Images, photographs, or waveform data
- Financial or payment information relating to patients
- Data concerning individuals who have not consented, whose consent has been withdrawn, or who have opted out of research or secondary use
- Data subject to a legal hold, a research protocol restriction, or a data use agreement whose terms conflict with the Business Associate Agreement
- Data subject to 42 C.F.R. Part 2 (substance use disorder records) unless the Hospital has told us in writing and we have executed the additional agreement Part 2 requires

Use pseudonymous sample identifiers. A sample identifier that encodes a medical record number, initials, or a date of birth defeats the purpose. The Service accepts any identifier string; the Hospital chooses what it means. Bioprium does not hold, and does not want, the re-identification key.

If a Hospital sends data in these categories anyway, see Section 21.4.

---

6. CONSENT AND AUTHORIZATION — HOSPITAL OBLIGATIONS

This section is the core of the allocation of responsibility between Bioprium and the Hospital. Read it in full.

6.1 The Hospital obtains consent. We do not.

Bioprium has no relationship with the patient. We do not meet the patient, do not counsel the patient, do not present a consent form, and have no independent means of verifying what any patient was told. **The Hospital is the party in the room. The Hospital obtains the consent.**

6.2 Hospital representations and warranties

By submitting Hospital Data to the Service, the Hospital **represents, warrants, and covenants**, on each and every submission, that:

(a) Lawful authority. It has full legal right, power, and authority to disclose the Hospital Data to Bioprium and to instruct Bioprium to process it as contemplated by the Business Associate Agreement and this policy.

(b) HIPAA compliance. The disclosure is permitted under the HIPAA Privacy Rule, and the Hospital has satisfied any requirement for patient authorization under 45 C.F.R. § 164.508, or has determined that the disclosure falls within a permitted use or disclosure for treatment, payment, or healthcare operations under 45 C.F.R. § 164.502 and § 164.506.

(c) Informed consent for genomic analysis. Where the applicable analysis constitutes genetic testing, predictive genetic testing, or research under any applicable federal, state, tribal, foreign, institutional, or professional

standard, the Hospital has obtained **specific, written, informed consent** from the patient or the patient's legally authorized representative, and that consent:

1. is specific to genomic sequencing and analysis of the type performed;
2. discloses that data will be transmitted to and processed by a **third-party vendor**;
3. where the analysis may reveal predictive information about an untreatable or currently incurable condition — including Huntington's disease — complies with the heightened standards described in Section 12;
4. addresses the disposition of incidental and secondary findings;
5. addresses whether de-identified data may be used for product improvement, method validation, and research, if the Hospital has permitted such use; and
6. has not been withdrawn, revoked, or limited as of the moment of submission.

(d) Notice of Privacy Practices. Its Notice of Privacy Practices, as required by 45 C.F.R. § 164.520, accurately describes disclosures to business associates for the purposes for which Hospital Data is submitted.

(e) Institutional review. Where the processing constitutes human subjects research under 45 C.F.R. Part 46 or 21 C.F.R. Parts 50 and 56, the Hospital has obtained approval from a duly constituted Institutional Review Board or Privacy Board, or a documented determination of exemption or waiver, and is in compliance with that approval's conditions.

(f) Minimum necessary. It has applied the minimum necessary standard under 45 C.F.R. § 164.502(b) and has not disclosed more PHI than is required for the purpose.

(g) Genetic privacy statutes. It has complied with every applicable state genetic privacy statute, including but not limited to informed-consent, written-authorization, sample-retention, and destruction requirements under Alaska, Colorado, Florida, Georgia, Illinois, Louisiana, Massachusetts, Minnesota, Nevada, New Jersey, New Mexico, New York, Oregon, South Dakota, Texas, Utah, and Vermont law, and any comparable law of any other jurisdiction.

(h) No prohibited data. The Hospital Data does not include categories excluded under Section 5.6.

(i) Withdrawal. It maintains a process by which a patient may withdraw consent, and it will notify Bioprium and issue a deletion instruction promptly upon any withdrawal that affects data held by Bioprium.

(j) Accuracy of instruction. Every instruction it gives Bioprium regarding Hospital Data is lawful.

6.3 Allocation of responsibility for consent failures

Bioprium is entitled to rely conclusively on the Hospital's representations in Section 6.2, without independent investigation or verification. We have no practical ability to audit a consent form we have never seen, executed by a patient we have never met, in a clinical encounter at which we were not present. The party that can verify consent is the party that obtained it.

Accordingly, and to the maximum extent permitted by applicable law:

(a) The Hospital is solely responsible for obtaining, documenting, maintaining, honoring, and — where required — revoking patient consent and authorization.

(b) Bioprium bears no responsibility for, and disclaims all liability arising from, any failure of the Hospital to obtain adequate consent or authorization; any defect, insufficiency, expiration, revocation, or invalidity of any consent or authorization; any misrepresentation to a patient regarding the use or disclosure of their data; any breach by the

Hospital of its Notice of Privacy Practices; any failure to comply with an IRB determination; or any use of Hospital Data outside the scope of the consent obtained.

(c) The Hospital shall **indemnify, defend, and hold harmless** Bioprium and its officers, directors, employees, agents, successors, and assigns from and against any and all claims, demands, actions, causes of action, proceedings, investigations, liabilities, losses, damages, fines, penalties, settlements, judgments, and expenses (including reasonable attorneys' fees, expert fees, and costs of investigation and defense) arising out of or relating to any breach of the representations and warranties in Section 6.2 — including, without limitation, any claim brought by a patient, a patient's family member, a patient's estate, a class of patients, a state attorney general, or any regulator, alleging that the patient's data was collected, used, or disclosed without proper consent or authorization.

(d) This allocation survives termination of the Hospital's account, subscription, Business Associate Agreement, and Master Services Agreement.

6.4 What this allocation does NOT do — and why we say so

We want to be direct with you, because a Hospital's counsel will identify this immediately and it is better that you hear it from us.

The allocation in Section 6.3 governs the relationship **between Bioprium and the Hospital**. It is a contractual allocation of risk between two commercial parties, and as such it is generally enforceable between them.

It does **not**, and cannot:

- **Eliminate Bioprium's direct liability under HIPAA.** Since the HITECH Act of 2009 and the 2013 Omnibus Rule, business associates are directly liable to the Department of Health and Human Services Office for Civil Rights for violations of the Security Rule, for impermissible uses and disclosures, and for specified Privacy Rule provisions. Civil monetary penalties can be imposed on Bioprium directly. **No contract with a Hospital and no privacy policy on a website can contract that away**, because the obligation runs to the government, not to the Hospital.
- **Bind patients or third parties.** A patient is not a party to this policy or to the Business Associate Agreement. A patient who believes their data was misused may name Bioprium as a defendant regardless of what Bioprium and the Hospital agreed between themselves. What the allocation does is determine who ultimately bears the cost — through indemnification — after the fact.
- **Displace state statutes that create direct duties.** Several state genetic privacy laws impose duties on any person or entity holding genetic information, not solely on the entity that collected it. Washington's My Health My Data Act creates a private right of action exercisable against a "regulated entity."
- **Survive Bioprium's own misconduct.** No allocation protects Bioprium from liability for its own breach, negligence, or willful misconduct, and this policy does not purport to create one.

The practical conclusion: consent allocation is necessary but not sufficient. Bioprium's actual protection comes from the combination of (i) the contractual allocation above, (ii) an executed Business Associate Agreement with clear scope, (iii) genuine technical and organizational safeguards, and (iv) insurance. Bioprium maintains cyber liability and technology errors-and-omissions insurance with [CARRIER], at limits of [LIMITS].

6.5 Bioprium's own obligations

We do not treat Section 6.3 as license to be careless. Independently of the Hospital's obligations, Bioprium will:

- Use and disclose PHI only as permitted by the Business Associate Agreement and this policy;

- Not use or disclose PHI in a manner that would violate the Privacy Rule if done by a Covered Entity, except as permitted at 45 C.F.R. § 164.504(e)(2)(i)(A);
- Implement the administrative, physical, and technical safeguards required by the Security Rule at 45 C.F.R. §§ 164.308, 164.310, 164.312, and 164.316;
- Bind every Subprocessor to equivalent restrictions in writing;
- Report breaches of unsecured PHI as required by 45 C.F.R. § 164.410, and security incidents as required by 45 C.F.R. § 164.314(a)(2)(i)(C) and Section 22;
- Make available our books, records, and practices to HHS as required at 45 C.F.R. § 164.504(e)(2)(ii)(I);
- Return or destroy PHI at termination as required at 45 C.F.R. § 164.504(e)(2)(ii)(J);
- Refuse an instruction from a Hospital that we know or reasonably believe to be unlawful, and notify the Hospital.

---

7. HOW DATA IS COLLECTED

7.1 Hospital Data collection channels

Available today — local software distribution. The Hospital operates the software itself, natively or in a container. Bioprium receives nothing.

In development — on-premise or in-VPC deployment. The Service runs inside the Hospital's own environment. Hospital Data never leaves the Hospital's infrastructure and Bioprium never receives it. This is the deployment we recommend for identifiable patient data.

The three channels below are **not yet built**. They are planned for the Production Service and are described here so that a Hospital evaluating us can see what is coming and what is not:

- **Authenticated upload** — Hospital-authenticated transfer over TLS 1.2 or higher into a per-tenant, encrypted storage location.
- **Pull from a Hospital-controlled endpoint** — Bioprium retrieves data from a location the Hospital designates and controls, using credentials the Hospital issues and can revoke. We prefer this, because the Hospital keeps the ability to cut off access unilaterally.
- **Direct integration** — SFTP, S3-compatible object storage, or API integration, configured per Hospital.

We do not collect Hospital Data by scraping, by purchase, by brokerage, or from any source other than the Hospital that submits it or an endpoint that Hospital designates.

7.2 Website and account data collection

Described in Section 8.

---

8. ACCOUNT, BILLING, AND WEBSITE DATA

This is Tier Two data, for which Bioprium is the controller.

8.1 Account registration

To create an account or purchase a subscription we collect: name; work email address; employer or institutional affiliation; job title or role; telephone number (optional); and authentication credentials. Passwords are stored only as salted hashes using a memory-hard algorithm. Where single sign-on or multi-factor authentication is used, we store the associated identifiers and factors.

8.2 Subscription and billing

Payment card data is collected and processed **by our payment processor, [PAYMENT PROCESSOR]**, and is never transmitted to or stored on Bioprium systems. We receive and retain: billing contact, billing address, the last four digits and brand of the payment instrument, transaction identifiers, subscription tier, billing history, and tax identifiers. Retention of billing records is governed by tax and accounting law rather than by user request — see Section 20.4.

8.3 Usage and telemetry

For the Production Service we collect: authentication events; feature usage; API call metadata; job submission and completion events; error and exception traces; performance metrics; and audit logs of access to Hospital Data.

Audit logs of access to Hospital Data are themselves treated as PHI, because the fact that a specific sample was accessed at a specific time by a specific user is information about an individual's healthcare.

Diagnostic telemetry is configured to exclude genomic sequence content. Where an error trace could contain a fragment of Hospital Data, it is routed to the Hospital's tenant-isolated log store rather than to Bioprium's general telemetry pipeline.

8.4 Website and marketing data

From website visitors we collect: IP address; browser and device characteristics; referring URL; pages viewed and time on page; and information submitted through contact, demo-request, or newsletter forms.

Cookies and similar technologies. Our current use is described at [COOKIE POLICY URL]. We use strictly necessary cookies for session management and security. Beyond strictly necessary cookies we use [LIST ANY ANALYTICS OR ADVERTISING TECHNOLOGIES, OR STATE THAT YOU USE NONE].

A specific warning about pixels on health-related pages. The Federal Trade Commission has brought a series of enforcement actions against health and health-adjacent companies for deploying third-party advertising and analytics trackers on pages from which a visitor's health condition can be inferred, and the FTC and the HHS Office for Civil Rights have jointly issued warning letters on the practice. It is also the subject of extensive private class-action litigation and state attorney general activity. A visitor reading a page about Huntington's disease analysis has revealed something about themselves or a family member. **Bioprium does not deploy advertising trackers, advertising pixels, or third-party session-recording tools on disease-specific pages of its website, and does not sell or share website visitor data for cross-context behavioral advertising.**

8.5 Communications

We retain correspondence with you, including support tickets, sales correspondence, and recorded or transcribed calls where you have been notified and, where required by law, have consented.

---

9. WHAT WE DO NOT COLLECT

For the avoidance of doubt, Bioprium does **not**:

- Collect data directly from patients or consumers in a personal capacity;
- Operate a direct-to-consumer genetic testing service;
- Purchase, license, or otherwise acquire personal data or genomic data from data brokers;
- Sell personal information or Consumer Health Data, as "sell" is defined under the CCPA/CPRA, the Washington My Health My Data Act, Nevada SB 370, or any other applicable statute;
- Share personal information for cross-context behavioral advertising;
- Use Hospital Data for advertising, marketing, or targeting of any kind;
- Collect biometric identifiers as defined under the Illinois Biometric Information Privacy Act (fingerprints, voiceprints, retina or iris scans, hand or face geometry). **Note:** genomic data is not a BIPA biometric identifier, but it is regulated by other Illinois statutes including the Genetic Information Privacy Act, 410 ILCS 513 — which does carry a private right of action;
- Retain physical biological specimens. We process digital sequence data only.

---

10. PURPOSES OF PROCESSING

10.1 Hospital Data — permitted purposes

We process Hospital Data **only** to:

1. Provide the Service the Hospital has requested — ingest, quality control, genotyping, guide design, off-target analysis, structural assessment, and dossier generation;
2. Return outputs to the Hospital;
3. Maintain provenance and audit records required for traceability and regulatory defensibility;
4. Diagnose and resolve errors, at the Hospital's request or where necessary to restore service;
5. Maintain security, detect and investigate incidents, and prevent fraud and abuse;
6. Meet legal, regulatory, and contractual obligations;
7. Perform data aggregation services relating to the Hospital's own healthcare operations, as permitted at 45 C.F.R. § 164.504(e)(2)(i)(B);
8. Create De-identified Data, **only where the Business Associate Agreement expressly permits it** — see Section 15.

10.2 What we will not do with Hospital Data

We will not, and our Business Associate Agreement will prohibit us from:

- Using Hospital Data to train, fine-tune, evaluate, or benchmark machine learning models **in identifiable form**;
- Disclosing Hospital Data to any party other than the Hospital, an authorized user, or a contractually bound Subprocessor;

- Using one Hospital's data to provide services to another Hospital, except through De-identified or Aggregate Data where expressly permitted;
- Selling, renting, licensing, or brokering Hospital Data under any circumstances;
- Using Hospital Data for advertising or marketing;
- Combining Hospital Data with data from other sources to enrich, augment, or re-identify it;
- Transmitting patient-derived sequence to any public or third-party computational service — see Section 16.3.

---

11. LEGAL BASES FOR PROCESSING (GDPR / UK GDPR)

Where the EU or UK GDPR applies, Bioprium processes personal data on the following bases:

For **Hospital Data**, Bioprium is a processor and the Hospital's own basis applies. For health and genetic data under Article 9 that is ordinarily Art. 9(2)(a) explicit consent or Art. 9(2)(h) provision of healthcare, with Art. 6(1)(b) or Art. 6(1)(c) as the Article 6 basis. The Hospital, as controller, is responsible for establishing and documenting that basis.

For everything below, Bioprium is the controller:

- **Account and subscription data** — Art. 6(1)(b), performance of a contract.
- **Security, fraud prevention, and service improvement** — Art. 6(1)(f), legitimate interests, balanced against your rights.
- **Marketing communications** — Art. 6(1)(a) consent, or Art. 6(1)(f) for existing business contacts, always with an opt-out.
- **Legal and regulatory compliance** — Art. 6(1)(c), legal obligation.

Genetic data is a special category under Article 9(1). Where Bioprium processes it as a processor, the Article 9 condition is the Hospital's to establish.

---

12. GENETIC INFORMATION — SPECIAL HANDLING

Genomic data is not ordinary health data, and we do not treat it as such. This section exists because the risks it describes are real, are not adequately covered by generic health-privacy language, and — in the case of the Huntington's disease analysis Bioprium performs — are among the most serious in all of clinical genetics.

12.1 Why genomic data is categorically different

It is permanent. A compromised password can be changed. A compromised genome cannot. A disclosure today is a disclosure for the rest of the individual's life.

It is shared. An individual's genome is substantially shared with their parents, siblings, and children. A disclosure about one person is a partial disclosure about their entire biological family — including relatives who never consented to anything, who may not know the testing occurred, and who may not wish to know their own risk.

It is identifying. Contemporary research has repeatedly demonstrated that genomic datasets described as de-identified can be re-identified — through surname inference from Y-chromosome markers combined with genealogy databases, through matching against public genotype resources, through long-range familial matching in

consumer genealogy databases, and through combination with demographic quasi-identifiers. **We do not represent that any genomic dataset is permanently and irreversibly anonymous, and we would treat any vendor who made that representation with suspicion.**

It is predictive. Genomic data speaks to future health, not only present health. That is what makes it clinically valuable and what makes its disclosure uniquely damaging.

12.2 The Huntington's disease analysis — heightened obligations

Bioprium's repeat-expansion analysis measures CAG repeat length at the *HTT* locus and classifies the result into penetrance bands. **A result in the fully penetrant range is, in effect, a prediction that the individual will develop Huntington's disease — a progressive, currently incurable, ultimately fatal neurodegenerative condition — if they live long enough.**

There is no category of information Bioprium handles that is more consequential. Accordingly:

(a) Heightened consent. Where a Hospital submits data for repeat-expansion analysis at the *HTT* locus or any comparable predictive locus, the Hospital warrants that it has obtained consent conforming to the current international recommendations for predictive genetic testing in Huntington's disease — **MacLeod et al., "Recommendations for the predictive genetic test in Huntington's disease," *Clinical Genetics* 2013;83:221–231**, issued by the European Huntington's Disease Network Genetic Testing and Counselling Working Group together with the International Huntington Association and the World Federation of Neurology, superseding the 1994 guidelines. These contemplate pre-test genetic counseling, a period for reflection between counseling and testing, results delivered in person by a qualified professional, and post-test support, and they address specifically the counseling of intermediate and reduced-penetrance results — **precisely the bands this Service reports.**

(b) Bioprium provides no counseling. We are not genetic counselors. We do not deliver results to patients. We do not contact patients. **A Bioprium output must never be delivered to a patient as a result without the involvement of a qualified clinician or genetic counselor.**

(c) Testing of minors. Predictive testing of asymptomatic minors for adult-onset conditions is contrary to the position of every major professional genetics body. Bioprium will not knowingly process data for predictive analysis at the *HTT* locus, or any comparable adult-onset predictive locus, where the Hospital has indicated the subject is a minor, absent documented clinical justification and review by an Institutional Review Board or ethics committee. See also Section 13.

(d) The right not to know. Individuals at risk for Huntington's disease have a well-recognized right not to learn their status. A substantial majority of at-risk individuals choose not to be tested. Analysis performed for an unrelated purpose can incidentally reveal repeat status. **The Hospital is responsible for ensuring that its consent process addresses incidental findings and honors a patient's stated preference not to receive them.** Bioprium returns outputs to the Hospital, not to the patient, precisely so that this decision stays with the clinician who obtained the consent.

(e) Family members. A repeat expansion identified in one individual carries a 50% transmission probability to each child and implies risk in a parent. **Bioprium does not contact, notify, or disclose to family members under any circumstance.** Whether and how to address familial implications is a clinical and ethical decision belonging to the Hospital.

12.3 Anti-discrimination law — what protects a patient, and what does not

We set this out because patients and Hospitals frequently overestimate the coverage of federal law.

The Genetic Information Nondiscrimination Act of 2008 (GINA) prohibits:

- Health insurers from using genetic information for eligibility, coverage, underwriting, or premium-setting (Title I);
- Employers with 15 or more employees from using genetic information in hiring, firing, promotion, compensation, or terms of employment, and from requesting or purchasing it (Title II).

GINA does NOT prohibit discrimination in:

- **Life insurance**
- **Disability insurance**
- **Long-term care insurance**
- Employment by employers with fewer than 15 employees
- Certain military contexts

This is the gap that matters most. An individual who learns they carry a fully penetrant *HTT* expansion may face refusal or repricing of life, disability, and long-term care insurance, and federal law does not prevent it. Some states — including California, Florida, Vermont, and others — have extended protections into these lines; most have not. Any consent process for predictive genetic testing that does not disclose this gap is, in our view, inadequate.

Other protections that may apply: the HIPAA Privacy Rule, which treats genetic information as PHI and prohibits health plans from using or disclosing it for underwriting purposes; the Americans with Disabilities Act, for manifested conditions; and state genetic privacy statutes, several of which impose consent, ownership, and destruction requirements stricter than federal law and several of which carry a private right of action.

Nothing in this policy is legal advice to any patient. A patient concerned about discrimination should consult a genetic counselor and, where warranted, an attorney, before undergoing predictive testing.

12.4 Our commitments regarding genetic information

Bioprium will:

- Treat all genomic data and Derived Data as sensitive personal information requiring the highest level of protection under every applicable framework;
- Never disclose genetic information to an insurer, employer, or their agent, except pursuant to a valid, specific patient authorization presented to us by the Hospital, or as compelled by law after the process in Section 16.5;
- Never use genetic information to make or support any decision about employment, insurance, credit, housing, or education;
- Never attempt to re-identify De-identified Data, and contractually prohibit our Subprocessors and De-identified Data recipients from doing so;
- Apply access controls that are specific to genomic data rather than inherited from general system permissions;
- Refuse to participate in familial searching, forensic genetic genealogy, or law enforcement genomic matching of any kind, and resist any demand to do so to the fullest extent the law allows.

---

13. CHILDREN'S AND PEDIATRIC DATA

Bioprium's Service is designed for clinical and research use in pediatric as well as adult populations, and an early target population is pediatric genomics. Pediatric genomic data therefore requires explicit treatment.

The website and account registration are not directed to children. We do not knowingly collect personal information from any individual under 18 through our website, and no one under 18 may create an account or purchase a subscription. If we learn we have collected such information, we will delete it.

Pediatric patient data submitted by a Hospital is a different matter. Where a Hospital submits data concerning a minor, the Hospital warrants that it has obtained consent or permission from a parent or legal guardian in accordance with 45 C.F.R. § 164.502(g) and applicable state law, and, where the minor is of sufficient maturity, has obtained assent in accordance with the applicable IRB determination or professional standard.

Bioprium applies the same technical protections to pediatric data as to adult data, and applies the additional restriction in Section 12.2(c) regarding predictive testing of minors.

State laws granting minors independent authority over certain categories of their own health records, and laws restricting parental access to those records, are the Hospital's to administer; Bioprium returns data to the Hospital and does not adjudicate access between a minor and a parent.

---

14. HOSPITAL RIGHTS AND CONTROLS

This section states what a Hospital gets. It is the counterpart to Section 6.

14.1 Ownership

The Hospital retains all right, title, and interest in and to its Hospital Data. Bioprium acquires no ownership interest in Hospital Data by virtue of processing it. Bioprium receives only a limited, non-exclusive, non-transferable, revocable license to process Hospital Data for the purposes in Section 10.1, for the term of the agreement.

Derived Data. Outputs generated from a Hospital's data — dossiers, guide candidates, off-target catalogs, genotype calls — belong to the Hospital, subject to Bioprium's retained rights in the underlying software, algorithms, methods, models, scoring functions, reference databases, and registries used to produce them. Bioprium claims no ownership of a patient's genotype and no ownership of the clinical conclusions a Hospital draws.

14.2 Access and portability

A Hospital may, at any time during the term:

- Access and export all of its Hospital Data and Derived Data in a standard, machine-readable format (BAM/CRAM/VCF for sequence data; JSON for structured outputs; HTML/PDF for rendered dossiers);
- Obtain a copy of the provenance records for any run;
- Obtain audit logs showing every access to its data, by whom, when, and from where;
- Obtain the current Subprocessor list and the applicable data flow documentation.

Export is available through the Service without charge and without a support request. We do not hold data hostage as a commercial lever.

14.3 Correction, amendment, and access requests

Bioprium will, within **[10] business days** of a written request:

- Make PHI available so the Hospital can respond to a patient's right of access under 45 C.F.R. § 164.524;
- Amend PHI as the Hospital directs, under 45 C.F.R. § 164.526;
- Provide an accounting of disclosures under 45 C.F.R. § 164.528;
- Provide the information the Hospital needs to respond to a request under any state comprehensive privacy law or the GDPR.

14.4 Deletion

A Hospital may instruct deletion of any dataset, any patient's data, or all of its data at any time. On receipt of a written deletion instruction, Bioprium will delete the specified data from production systems within **[30] days** and from backups within **[90] days** or on the expiry of the backup rotation, whichever is sooner, subject to Section 20.4.

Deletion instructions are honored without inquiry into the reason. We do not require a Hospital to explain a patient's withdrawal of consent.

14.5 Restriction and suspension

A Hospital may instruct Bioprium to restrict processing of a dataset, to suspend an integration, or to revoke credentials, and may do so unilaterally where the Hospital controls the source endpoint. Bioprium will comply promptly.

14.6 Audit rights

A Hospital may, on **[30] days'** written notice and no more than **[once per twelve-month period]** (or more frequently following a security incident affecting that Hospital, or where required by a regulator):

- Review Bioprium's written information security program, policies, and procedures;
- Receive completed security questionnaires;
- Review the results of Bioprium's most recent penetration test and vulnerability assessment;
- Review any third-party audit report Bioprium holds;
- Conduct an on-site or remote assessment, at the Hospital's expense, subject to reasonable confidentiality and safety conditions.

14.7 Subprocessor objection

Bioprium will give **[30] days'** advance notice before engaging a new Subprocessor that will process Hospital Data. A Hospital may object on reasonable, documented security or compliance grounds. If we cannot resolve the objection, the Hospital may terminate the affected service without penalty and receive a pro-rata refund of prepaid fees.

14.8 Termination and return

On termination, at the Hospital's election, Bioprium will return all Hospital Data in a standard format, or destroy it, and will certify the destruction in writing. Where return or destruction is infeasible, Bioprium will extend the

protections of this policy and the Business Associate Agreement to the retained data and limit further use to the purpose making return or destruction infeasible, as 45 C.F.R. § 164.504(e)(2)(ii)(J) requires. **We will identify specifically what was retained and why. "Infeasible" is not a general-purpose exception and we will not use it as one.**

14.9 Change of control

If Bioprium is acquired, merged, or has its assets sold, Hospital Data may transfer as part of the transaction. Bioprium will provide **[30] days'** notice, the successor will be bound by protections no less protective than these, and the Hospital may terminate and require deletion before the transfer completes.

---

15. OUR RIGHTS — DE-IDENTIFIED DATA AND AGGREGATE DATA

We are stating our own rights explicitly rather than burying them, because a vendor that hides its secondary-use rights in a definitions section is a vendor a hospital should not trust.

15.1 What we claim

Subject to the Business Associate Agreement and to any restriction a Hospital imposes, Bioprium reserves the right to:

(a) Create De-identified Data from Hospital Data, in accordance with 45 C.F.R. § 164.514(b), and to use and disclose that De-identified Data for: improving the Service; developing, validating, and benchmarking algorithms and models; scientific research and publication; quality assurance; and the development of new products and features.

(b) Generate and use Aggregate Data — statistics, benchmarks, performance metrics, and usage patterns — that do not identify any Hospital, patient, or individual.

(c) Retain and use all software, algorithms, methods, scoring functions, technology, know-how, and general knowledge developed or improved in the course of providing the Service, including improvements informed by working with Hospital Data.

(d) Retain provenance and audit records for the period required by Section 20, notwithstanding a deletion instruction, where retention is required by law or is necessary to demonstrate compliance.

15.2 What we do not claim

We do **not** claim, and this policy does not grant us:

- Any right to use identifiable Hospital Data for product development, model training, research, or any purpose beyond Section 10.1;
- Any right to de-identify Hospital Data **where the Business Associate Agreement does not permit it**. HIPAA permits a business associate to de-identify PHI only if the BAA authorizes it. **Absent that authorization, we will not do it.**
- Any ownership of a patient's genome or genotype;
- Any right to disclose De-identified Data in a manner that would permit or facilitate re-identification;
- Any right to sell De-identified Data derived from a Hospital's patients.

15.3 The limits of genomic de-identification

We will not tell you that de-identified genomic data is anonymous, because that is not true.

HIPAA Safe Harbor de-identification requires removal of eighteen enumerated identifier categories at 45 C.F.R. § 164.514(b)(2)(i)(A)–(R). **A genomic sequence is not among the enumerated categories** — the regulation predates routine whole-genome sequencing. Whether sequence is nonetheless captured by category (P), "biometric identifiers," or the residual category (R), "any other unique identifying number, characteristic, or code," has not been resolved by HHS, and we do not assume the favorable reading.

There is a second and more fundamental problem. Safe Harbor also requires, at § 164.514(b)(2)(ii), that the entity have **no actual knowledge** that the residual information could be used to identify the individual. Bioprium has stated its actual knowledge, at length, in Section 12.1. **A company that knows genomic data is re-identifiable cannot in good faith rely on Safe Harbor for genomic data.** We therefore do not.

Bioprium therefore applies the following in addition to Safe Harbor removal:

- **Expert Determination** under § 164.514(b)(1) for any genomic dataset released outside Bioprium, rather than reliance on Safe Harbor alone;
- Reduction to the minimum genomic interval necessary for the analytical purpose, rather than release of full sequence;
- Preference for release of derived summary statistics over release of sequence;
- Contractual prohibition on re-identification, on linkage to other datasets, and on onward transfer, binding every recipient;
- Access controls and data use agreements rather than open publication, for any dataset from which an individual could plausibly be recovered;
- No release of De-identified Data at all where the Business Associate Agreement does not permit it.

A Hospital may prohibit de-identification and secondary use entirely. That option is available in the Business Associate Agreement and choosing it does not affect pricing or service levels.

---

16. WHO CAN ACCESS DATA

16.1 Bioprium personnel

Access to Hospital Data is restricted to personnel with a documented business need, and is:

- **Role-based.** Access is granted by role, not by individual discretion, under the minimum necessary standard at 45 C.F.R. § 164.502(b) and § 164.514(d).
- **Least privilege.** The default is no access. Access to genomic data is a distinct, separately granted permission and is not inherited from general engineering or administrative privileges.
- **Authenticated.** Multi-factor authentication is required for all personnel access to any system that holds or can reach Hospital Data.
- **Logged.** Every access is recorded with actor, timestamp, source, dataset, and action. Logs are retained per Section 20 and are available to the Hospital under Section 14.2.
- **Reviewed.** Access rights are reviewed at least **[quarterly]** and revoked immediately on role change or separation.

- **Trained.** Personnel with access complete HIPAA and information-security training on hire and at least annually, and are bound by confidentiality obligations that survive employment.
- **Conditioned on background screening**, to the extent permitted by law, for roles with production access.

Emergency access. Where a production incident requires access to Hospital Data to restore service, a break-glass procedure applies: access is time-limited, requires a second-person approval, is logged as a distinct event type, and is reported to the affected Hospital within **[5] business days** with a description of what was accessed and why.

16.2 Subprocessors

Bioprium engages third parties to provide infrastructure and operational services. Each Subprocessor that may process Hospital Data:

- Is bound by a written agreement imposing obligations no less protective than those in this policy and the applicable Business Associate Agreement;
- Has executed a **Business Associate Agreement** with Bioprium where it may access PHI;
- Is assessed before engagement and periodically thereafter;
- Is permitted to process Hospital Data only to deliver its contracted service.

Current Subprocessor categories:

Subprocessors that may access PHI. Each is bound by a Business Associate Agreement with Bioprium:

- **Cloud infrastructure and storage** — hosting, compute, and encrypted object storage. Data is encrypted at rest. Provider: [PROVIDER — e.g., AWS / GCP / Azure, with regions].
- **Managed database** — structured data and registries. Provider: [PROVIDER].
- **Backup and disaster recovery** — encrypted backups. Provider: [PROVIDER].

Subprocessors that do not access PHI:

- **Error monitoring and observability** — diagnostics, configured to exclude Hospital Data. Provider: [PROVIDER].
- **Identity and access management** — authentication. Account data only, no PHI. Provider: [PROVIDER].
- **Payment processing** — subscription billing. No PHI. Provider: [PROVIDER].

Subprocessors with incidental exposure only:

- **Business email and productivity** — corporate communications. Provider: [PROVIDER].
- **Customer support** — ticketing, configured to discourage PHI submission. Provider: [PROVIDER].

A current and complete Subprocessor list, including entity names, processing locations, and BAA status, is maintained at **[SUBPROCESSOR PAGE URL]** and is available to any Hospital on request. Changes are notified under Section 14.7.

16.3 A specific commitment on third-party sequence services

Computational biology routinely relies on public academic web services — multiple sequence alignment servers, structure prediction endpoints, annotation APIs, variant databases. These services are valuable, free, and operated without any healthcare privacy commitment whatsoever. They have no Business Associate Agreement, no defined retention period, no breach notification duty, and in many cases explicitly log submitted queries.

Bioprium commits that no patient-derived sequence, and no data derived from a patient's sequence from which sequence could be reconstructed, is transmitted to any public or third-party computational service. Specifically:

- Multiple sequence alignment for structural analysis is performed against **reference and registry sequences only**, never against patient-derived sequence.
- Before the Production Service accepts PHI, Bioprium will operate its **own multiple-sequence-alignment infrastructure within its controlled environment**, eliminating the dependency on the public alignment endpoint used in the current research build.
- Off-target scanning, genotype calling, repeat sizing, and all other analyses that touch patient sequence run entirely within Bioprium-controlled or Hospital-controlled infrastructure.
- Reference data — genome assemblies, allele registries, repeat catalogs, scoring matrices, deposited structures — is downloaded into our environment and versioned ahead of analysis. We do not query external services with patient data at analysis time.
- The Service is configured so that the sequence-alignment toolchain does not fall back to a remote reference server when a local reference is absent. It fails instead. A silent remote fetch triggered by a missing local file is a disclosure, and we treat it as one.
- Structure prediction is not executed on rented third-party compute where patient-derived inputs are involved.

Two of these are commitments rather than descriptions of the current research build, and we will not blur the distinction. The research build (i) uses a public multiple-sequence-alignment endpoint, and (ii) contains a code path for dispatching structure prediction to a rented external GPU host. Both are acceptable today only because that build processes public reference data exclusively and no patient data. **Standing up self-hosted alignment infrastructure, and removing or hard-disabling the external-compute path, are conditions precedent to accepting PHI** — enforced in code by a refusal, not by a configuration default. See Section 1.

A note on the public-data acquisition scripts. Bioprium's benchmarking tooling retrieves public reference cohorts over the network, in some cases slicing a remote file in place using HTTP range requests. Those scripts operate exclusively on public consented reference cohorts and are not part of the patient-data pipeline. They are named here so that a reviewer reading the source does not mistake them for a patient egress path. A full network egress inventory is available to Hospitals on request.

16.4 Hospital users

Each Hospital administers its own users. Bioprium provides role-based access controls and audit logging; **the Hospital is responsible for provisioning, reviewing, and deprovisioning its own users' access, and for the actions of those users.** A Hospital's failure to deprovision a departed employee is not a Bioprium security incident.

16.5 Legal process and government demands

Bioprium may disclose data where compelled by valid legal process. Our practice:

- **We require valid process.** We do not disclose in response to an informal request. We require a subpoena, court order, warrant, or other legally valid demand, and we assess its validity and scope.
- **We notify.** We notify the affected Hospital before disclosure, with enough time to seek a protective order, **unless legally prohibited**. Where prohibited, we notify as soon as the prohibition lapses.
- **We narrow.** We object to demands that are overbroad, seek data beyond the requester's jurisdiction, or seek genomic data where a narrower response suffices.
- **We follow HIPAA.** Disclosures of PHI in response to legal process comply with 45 C.F.R. § 164.512(e) and (f), including the requirement for satisfactory assurances of notice or a qualified protective order.

- **We resist law enforcement genomic requests specifically.** Bioprium will not voluntarily provide genomic data or genotype information for forensic identification, familial searching, or investigative genetic genealogy, and will require a warrant and challenge overbroad demands.
- **We report.** Bioprium will publish an annual transparency report at **[URL]** stating the number of legal demands received, by category, and the number complied with, to the extent disclosure is permitted.

16.6 Other disclosures

Bioprium may also disclose data:

- To professional advisers (counsel, auditors, insurers) under confidentiality obligations;
- In connection with a merger, acquisition, financing, or asset sale, subject to Section 14.9, and with genomic data disclosed in diligence only in de-identified or aggregate form until closing;
- Where necessary to prevent imminent serious harm to health or safety, as permitted at 45 C.F.R. § 164.512(j);
- With the Hospital's written direction.

---

17. SECURITY

Bioprium maintains a written information security program addressing the administrative, physical, and technical safeguards required by the HIPAA Security Rule at 45 C.F.R. §§ 164.308, 164.310, 164.312, and 164.316.

> ***A note on the direction of travel.*** *HHS published a Notice of Proposed Rulemaking in January 2025 that would substantially strengthen the Security Rule — removing the "addressable" category so that nearly all specifications become required, and mandating encryption, multi-factor authentication, asset inventories, network segmentation, and regular vulnerability scanning and penetration testing. Publication of the final rule has been deferred, with a current target of 2027.* ***Bioprium's security program is being built to the proposed standard rather than the current minimum****, because the proposed standard is where the rule is going and because hospital security reviewers already expect it.*

17.1 Technical safeguards

- **Encryption in transit.** TLS 1.2 or higher for all connections, with modern cipher suites and certificate validation.
- **Encryption at rest.** AES-256 for all stored Hospital Data, including backups and archives, with keys managed in a dedicated key management service and rotated on a defined schedule.
- **Tenant isolation.** Each Hospital's data is logically isolated. Cross-tenant access is prevented at the storage, database, and application layers, and cross-tenant queries are structurally impossible rather than merely prohibited.
- **Authentication.** Multi-factor authentication is required for all Bioprium personnel and is available and recommended — **[or required]** — for all Hospital users. SAML/OIDC single sign-on is supported for Hospital identity providers.
- **Network controls.** Private networking, security groups, and segmentation between the processing environment and the general corporate environment.

- **Endpoint controls.** Full-disk encryption, endpoint detection and response, and centrally managed configuration on all devices that can reach production.
- **Vulnerability management.** Automated dependency scanning in continuous integration, container image scanning, and remediation targets of **[7 days for critical, 30 days for high]**.
- **Penetration testing.** Independent testing at least **[annually]** and after significant architectural change.
- **Logging and monitoring.** Centralized, tamper-evident logging with alerting on anomalous access patterns.
- **Secure development.** Code review on every change, automated test suites, secrets scanning, and separation of development, staging, and production. **No production Hospital Data is ever copied into a development, staging, test, or demonstration environment.**

17.2 Administrative safeguards

- Designated Privacy Official and Security Official (Section 2)
- Annual and event-driven risk analysis under 45 C.F.R. § 164.308(a)(1)(ii)(A)
- Documented risk management plan
- Workforce security, clearance, and termination procedures
- Security awareness and HIPAA training on hire and annually
- Incident response plan, tested at least annually
- Contingency, backup, and disaster recovery plans, with restoration tested at least **[annually]**
- Subprocessor due diligence and periodic reassessment
- Documentation retained for six years, per 45 C.F.R. § 164.316(b)(2)(i)

17.3 Physical safeguards

Bioprium operates no data centers. Physical security for infrastructure is provided by our cloud Subprocessors under their respective certifications. Bioprium's own facilities and devices are subject to access control, device encryption, clean-desk requirements, and secure media disposal.

17.4 Genomic-specific controls

Implemented today:

- Analysis intervals are constrained at ingestion on the short-read path, so that whole-genome data is not retained where a locus slice suffices
- Reference-server fallback is disabled, so a missing local reference fails rather than triggering a remote fetch
- Re-identification is contractually prohibited for Bioprium personnel, Subprocessors, and any recipient of De-identified Data

Committed for the Production Service, before PHI is accepted:

- Genomic data access as a distinct permission, separately granted and separately logged
- Elevated authorization and alerting on bulk export of genomic data
- Egress volume anomaly detection
- Extension of the ingestion validation and interval-constraint layer to the long-read path
- Blocking (non-silent) audit logging of all PHI access

We separate these two lists rather than presenting a single list in the present tense, because a security control described as existing when it does not is a misrepresentation, and because a Hospital deciding today deserves to know which is which.

17.5 The honest limitation

No system is perfectly secure, and we will not claim otherwise. Bioprium is an early-stage company with a small team. Our security program is real but it is young, and it has not yet been independently attested. We think a Hospital deciding whether to send us patient data deserves to know that, weigh it, and — if the risk is unacceptable today — choose the on-premise deployment in Section 7.1 instead, where their data never reaches us at all.

17.6 Vulnerability disclosure

Report suspected vulnerabilities to **security@[DOMAIN]**, encrypted with the key at **[URL]**. We commit to acknowledge within **[2] business days**, provide a substantive response within **[10] business days**, and not to pursue legal action against good-faith security research conducted in accordance with our disclosure policy at **[URL]**.

---

18. PATIENT AND CONSUMER RIGHTS

18.1 If you are a patient

Direct your request to your hospital or healthcare provider, not to Bioprium.

We understand this is frustrating, so here is the reason. Bioprium holds a sample identifier chosen by the Hospital and a genomic file associated with it. We do not hold your name, and we do not hold the key that maps the identifier to you. If you contacted us and asked “what data do you have about me,” **we could not answer the question without asking the Hospital to identify you to us — which would create a new disclosure of your identity to a company that currently does not have it.** That is worse for your privacy, not better.

Your hospital, as the Covered Entity, holds your rights under HIPAA: the right to access your records under 45 C.F.R. § 164.524, to request amendment under § 164.526, to an accounting of disclosures under § 164.528, to request restrictions under § 164.522, and to receive their Notice of Privacy Practices under § 164.520. Your hospital can compel us to act, and Section 14.3 obligates us to respond to them.

If you are unable to get a response from your hospital, or you believe your data reached Bioprium without your consent, contact us at **privacy@[DOMAIN]** anyway. We will not ignore you. We will work with the Hospital to resolve it, and if we conclude data was submitted without proper authority we will suspend processing and issue a deletion instruction.

You may also file a complaint with the HHS Office for Civil Rights at https://www.hhs.gov/ocr/complaints, with your state attorney general, or, where applicable, with a state privacy regulator such as the California Privacy Protection Agency.

18.2 If you are an account holder, a website visitor, or a business contact

For Tier Two data, Bioprium is the controller and you can come to us directly. Subject to verification and to applicable law, you may request:

- **Access / know** — confirmation of whether we process your personal information, and a copy
- **Correction** — rectification of inaccurate information
- **Deletion** — erasure, subject to Section 20.4
- **Portability** — a copy in a structured, commonly used, machine-readable format
- **Opt out of sale or sharing** — we do not sell or share personal information, but the right is available
- **Opt out of targeted advertising** — we do not conduct targeted advertising
- **Limit use of sensitive personal information** — under the CPRA
- **Opt out of profiling** with legal or similarly significant effects — we do not conduct such profiling
- **Withdraw consent** where processing is consent-based
- **Non-discrimination** — we will not deny service, charge different prices, or provide a different quality of service because you exercised a right
- **Appeal** — where a state law provides an appeal right, you may appeal a denial by writing to **privacy@[DOMAIN]** with "Privacy Appeal" in the subject line; we will respond within the statutory period and, if we deny the appeal, provide the contact details of your state attorney general
- **Object** or **restrict processing**, under the GDPR
- **Lodge a complaint** with a supervisory authority, under the GDPR

How to make a request: email **privacy@[DOMAIN]**, or use the form at **[URL]**, or call **[TOLL-FREE NUMBER]**.

Verification: we will verify your identity proportionately to the sensitivity of the request. We may decline a request we cannot verify.

Timing: we respond within **45 days**, extendable once by a further 45 days with notice, or within **one month** under the GDPR, extendable by two months.

Authorized agents: an authorized agent may submit a request on your behalf with written authorization and, where required, a power of attorney; we may contact you to confirm.

---

19. STATE-SPECIFIC DISCLOSURES

19.1 California — CCPA / CPRA

Categories of personal information collected in the preceding 12 months (Tier Two): identifiers; commercial information; internet or network activity; professional or employment-related information; and, where an account holder provides it, geolocation inferred from IP address.

Sensitive personal information: account credentials. In Tier One, Bioprium processes **genetic data**, which is sensitive personal information under Cal. Civ. Code § 1798.140(ae) — but does so **as a service provider**, not as a business, and only on the Hospital's instruction.

Sources: you; your employer; your interactions with our website and Service.

Business purposes: as stated in Section 10.

Disclosure for a business purpose: to the Subprocessor categories in Section 16.2.

Sale or sharing: Bioprium does not and has not sold or shared personal information, including the personal information of consumers under 16 years of age.

Use of sensitive personal information: limited to purposes permitted at Cal. Civ. Code § 1798.121(a) and 11 C.C.R. § 7027(m). We do not use or disclose sensitive personal information to infer characteristics.

Retention: as stated in Section 20.

HIPAA exemption: PHI processed under HIPAA is exempt from the CCPA under Cal. Civ. Code § 1798.145(c). **That exemption is data-level, not entity-level.** Bioprium's non-PHI data remains subject to the CCPA and we treat it accordingly.

Shine the Light: Cal. Civ. Code § 1798.83 — we do not disclose personal information to third parties for their direct marketing purposes.

CMIA: Bioprium is not a provider of health care, health care service plan, contractor, or corporation organized for the purpose of maintaining medical information as defined under the California Confidentiality of Medical Information Act, Cal. Civ. Code § 56 et seq.

19.2 Virginia, Colorado, Connecticut, Texas, Utah, Oregon, Montana, Delaware, Iowa, Nebraska, New Hampshire, New Jersey, Tennessee, Minnesota, Maryland, Indiana, Kentucky, Rhode Island, Florida, and other comprehensive state privacy laws

Bioprium acts as a **processor** for Hospital Data and as a **controller** for Tier Two data. Genetic data is **sensitive data** under each of these statutes and generally requires opt-in consent — **which the Hospital, as controller, obtains.** Rights and the appeal mechanism are as described in Section 18.2.

Texas residents: the notices required by Tex. Bus. & Com. Code § 541.102(b) and (c) are inapplicable because **we do not sell sensitive personal data or biometric personal data**. Bioprium's duties as a processor are governed by § 541.104. **Maryland** residents: the Maryland Online Data Privacy Act imposes a strict data-minimization standard and prohibits the sale of sensitive data outright; we do not sell sensitive data. **Minnesota** residents: you have the right to question the result of profiling; we do not engage in profiling that produces legal or similarly significant effects.

19.3 Washington, Nevada, and Connecticut — consumer health data

The **Washington My Health My Data Act** (RCW 19.373), the **Nevada Consumer Health Data Privacy Law** (SB 370, codified at NRS 603A.400 *et seq.*), and Connecticut's health-data amendments regulate "consumer health data" broadly and reach beyond HIPAA.

Washington's exemptions are data-level. MHMDA exempts PHI itself, but contains no entity-level HIPAA carve-out. Bioprium is therefore not exempt as an entity merely because much of what it handles is PHI. Non-PHI data collected through our website that reveals or is reasonably linkable to a health condition — for example, a demo request submitted from a page about Huntington's disease analysis — can constitute regulated consumer health data, and we treat it as such.

Nevada's exemption is structured differently. NRS 603A.490(1) excludes any person or entity subject to HIPAA and its implementing regulations, which is generally read as an entity-level exclusion. Bioprium may therefore fall outside Nevada's consumer health data law once it operates as a Business Associate. **We do not rely on that exclusion, and we extend the commitments below to Nevada consumers as a matter of policy regardless of whether the statute compels it.**

Accordingly:

- Bioprium **does not sell consumer health data**. The Washington statute requires a separate, signed "valid authorization" for any sale; we do not seek one because we do not sell.
- Bioprium **does not use a geofence** around any healthcare facility. RCW 19.373.080 prohibits implementing a geofence around an entity providing in-person healthcare services in order to identify or track consumers seeking care, collect their consumer health data, or send them health-related advertising; RCW 19.373.010 sets the relevant radius at 2,000 feet. We do not do this and have no plans to.
- Washington and Nevada consumers may request access to, and deletion of, their consumer health data, and may withdraw consent, by writing to **privacy@[DOMAIN]**.
- Our **Consumer Health Data Privacy Policy** is available at **[URL]**. RCW 19.373.020(2) requires a regulated entity to prominently publish a link to it on its homepage; Washington Attorney General guidance states that this must be a separate and distinct link rather than a section within another policy.

The Washington statute carries a private right of action through the Washington Consumer Protection Act. This is the single largest consumer-privacy litigation exposure Bioprium faces from its website, independent of anything to do with patient data.

19.4 Illinois

The **Illinois Genetic Information Privacy Act**, 410 ILCS 513, restricts disclosure of genetic testing information, prohibits its use by employers and insurers, and **provides a private right of action with statutory damages**. Where Bioprium processes data concerning Illinois residents it complies with GIPA in addition to HIPAA. Bioprium does not collect biometric identifiers as defined under BIPA, 740 ILCS 14.

19.5 Other state genetic privacy statutes

A number of states impose requirements exceeding federal law, including: property rights in genetic material and information; written informed consent specific to genetic testing; mandatory destruction of samples and data after a defined period; restrictions on disclosure even in de-identified form; and extension of anti-discrimination protection to life, disability, and long-term care insurance. States with statutes of this kind include Alaska, Colorado, Florida, Georgia, Louisiana, Massachusetts, Minnesota, Nevada, New Jersey, New Mexico, New York, Oregon, South Dakota, Texas, Utah, and Vermont, among others.

Determining which state's genetic privacy law applies to a given patient is the Hospital's responsibility, because the Hospital knows where the patient is and Bioprium does not. The Hospital warrants compliance under Section 6.2(g).

19.6 42 C.F.R. Part 2

Substance use disorder treatment records from Part 2 programs carry protections stricter than HIPAA, including consent requirements for redisclosure and a prohibition on use in legal proceedings absent a court order. The 2024 final rule aligning Part 2 more closely with HIPAA carried a compliance date of February 16, 2026.

Bioprium does not knowingly accept Part 2 records. A Hospital intending to submit data subject to Part 2 must notify Bioprium in writing in advance so the additional required agreements can be executed. Submission of Part 2 data without notice is a breach of Section 6.2(h).

19.7 Nevada SB 220 and other opt-out statutes

Nevada residents may direct a covered operator not to sell their covered information. Bioprium does not sell covered information. Requests: **privacy@[DOMAIN]**.

---

20. RETENTION AND DELETION

20.1 Principle

We retain data for the shortest period consistent with the purpose for which it was collected, the Hospital's instructions, and legal requirements. **Genomic data is retained on the shortest schedule of anything we hold**, because its risk profile does not decay.

20.2 Schedule

Genomic data and analysis artifacts. Submitted whole-genome files, where a slice is produced, are deleted within [7] days of successful slice production — there is no reason to keep them. Other submitted genomic sequence files are held for [30] days after analysis completion and output delivery, or for whatever shorter period the Hospital instructs. Sliced analysis intervals are held for [90] days, or as the Hospital instructs. Generated construct and sequence files are held with Derived Data, and filenames containing sample identifiers are renamed on redaction. Derived Data and dossiers are held for the term of the Hospital's subscription, or as the Hospital instructs.

Records we are required to keep. Provenance records and audit logs of PHI access are held for [6] years, as 45 C.F.R. § 164.316(b)(2)(i) requires. Provenance records are redacted on deletion in the manner described in Section 20.3. Run event logs are held for [6] years on the same redaction basis. Ingestion records — source filename, digest, and sample identifier — are held with the provenance record and redacted with it.

Business records. Account and subscription records are held for the term of the relationship plus [7] years for tax and accounting purposes. Billing records are held for [7] years. Support correspondence is held for [3] years. Website analytics are held for [13] months. Marketing contacts are held until opt-out plus [30] days, so that we can honor suppression.

Backups run on a [35] day rolling cycle. Deleted data ages out within one full rotation.

Hospitals may set shorter periods contractually. Shorter is better and we will accommodate it.

20.3 Provenance retention and the deletion tension

There is a genuine conflict here and we would rather name it than paper over it. Provenance records must be kept for six years to satisfy HIPAA documentation requirements and to make outputs auditable — but those records contain SHA-256 digests of patient files, which are PHI.

Our resolution: when Hospital Data is deleted, the corresponding provenance record is **redacted rather than destroyed**. Input file digests, sample identifiers, source filenames, and any other patient-linked field are removed; the tool versions, reference build, configuration digest, software commit, and run timestamp are retained. What survives establishes that a run occurred and on what software basis. What is removed is anything that connects it to a person.

A known architectural constraint, disclosed rather than glossed. Bioprium's design registry — the component that makes design provenance trustworthy — is **append-only by construction**. It has no delete or prune operation, deliberately, because mutable provenance is not provenance. Its records currently include a payload carrying the sample identifier and input digest. **Reconciling append-only provenance with a deletion obligation requires an architectural change, and completing that change is a condition precedent to the Production Service accepting PHI.** The intended resolution is to store patient-linked fields separately from the immutable design record, under a per-run key that can be destroyed — cryptographic erasure of the link rather than mutation of the ledger. Until that is built and verified, Bioprium cannot honor a deletion instruction against this component, and it will not accept PHI into it. Hospitals evaluating Bioprium today should treat this as an open item and ask for its status.

20.4 When we cannot delete

We may retain data notwithstanding a deletion request where retention is required to:

- Comply with a legal obligation, including HIPAA documentation and tax retention;
- Comply with a litigation hold, subpoena, or regulatory investigation;
- Establish, exercise, or defend legal claims;
- Detect and prevent security incidents and fraud;
- Complete a transaction you requested;
- Maintain the integrity of encrypted backups until they age out on the normal rotation.

Where we retain on one of these grounds we will tell you the ground, restrict processing to that purpose alone, and delete when the ground lapses.

20.5 Method

Deletion means cryptographic erasure of encryption keys together with logical deletion of the ciphertext, and secure overwriting where the storage medium supports it. Physical media disposal follows NIST SP 800-88 guidelines. Certificates of destruction are available to Hospitals on request.

---

21. DATA LOCATION AND INTERNATIONAL TRANSFERS

21.1 Where data is stored

Hospital Data submitted to the Production Service is stored and processed in **[REGION — e.g., United States, in AWS us-east-1 and us-west-2]**. Backups are stored in **[REGION]**. **Genomic data does not leave the United States** unless a Hospital specifically contracts for processing in another region.

Data residency options: Bioprium currently offers processing in [REGION(S)]. A Hospital that requires processing in a particular jurisdiction should raise it before contracting.

Account, billing, and website data may be processed in **[REGIONS]** by the Subprocessors listed in Section 16.2.

21.2 Transfer mechanisms

Where personal data is transferred from the EEA, the UK, or Switzerland to a country without an adequacy decision, Bioprium relies on the European Commission's **Standard Contractual Clauses** (Decision 2021/914),

together with the **UK International Data Transfer Addendum** where applicable, and conducts a transfer impact assessment. A copy of the executed clauses is available to Hospitals on request.

21.3 Genomic sovereignty

Several jurisdictions restrict cross-border transfer of human genomic data as a matter of national policy, independent of general data protection law — including, among others, China, Russia, India, and a number of countries with national biobank legislation. **A Hospital outside the United States must satisfy itself that transfer of genomic data to Bioprium is lawful in its jurisdiction before submitting anything.** Bioprium does not undertake that analysis for the Hospital and does not warrant that transfer is lawful in any particular country.

21.4 Unsolicited and inadvertent disclosures

If Bioprium receives PHI, identifiable genomic data, or other sensitive data it did not solicit and is not contracted to process — including by email, support ticket, misdirected upload, or submission before a Business Associate Agreement is executed — we will:

1. Not process, analyze, or further use it;
2. Isolate it and restrict access;
3. Notify the sending organization within **[2] business days**;
4. Securely destroy it within **[10] business days** unless the sender directs otherwise and an agreement is executed;
5. Document the event.

Receipt of unsolicited PHI does not create a Business Associate relationship, does not constitute acceptance of any obligation to process, and does not waive Section 1.4.

---

22. SECURITY INCIDENTS AND BREACH NOTIFICATION

22.1 To Hospitals

Bioprium will report to the affected Hospital:

- **Any breach of unsecured PHI**, without unreasonable delay and in no case later than **[30] days** — and, as a matter of practice, within **[5] business days** — after discovery, as required by 45 C.F.R. § 164.410. Bioprium's Business Associate Agreement will commit to the shorter period so the Hospital can meet its own 60-day obligation to individuals under § 164.404.
- **Any successful unauthorized access, use, disclosure, modification, or destruction** of Hospital Data, whether or not it meets the definition of a breach, within **[5] business days**.
- **Any ransomware or malware incident** affecting systems that hold Hospital Data, within **[24] hours** of discovery. Consistent with OCR guidance, ransomware affecting PHI is presumed to be a breach unless a low probability of compromise is demonstrated through a four-factor risk assessment.

Security incident reporting is required of Business Associates by 45 C.F.R. § 164.314(a)(2)(i)(C). **Unsuccessful attempts** — routine scanning, blocked intrusion attempts, failed logins — are reported in aggregate in periodic security reporting rather than individually. This treatment follows HHS commentary in the Security Rule preamble

(68 FR 8334, 8346) and subsequent OCR guidance rather than the text of the regulation, and it will be specified expressly in the Business Associate Agreement so that both parties are agreed on it.

22.2 Contents of a notification

To the extent known, and supplemented as the investigation proceeds: the date of the incident and of discovery; a description of what occurred; the categories and volume of data involved; the individuals or samples affected, identified to the Hospital by sample identifier; whether genomic sequence was involved; steps taken to contain and remediate; and the information the Hospital needs to meet its own notification obligations under 45 C.F.R. § 164.404 and applicable state breach law.

Where genomic data is involved, we will say so explicitly and prominently. Genomic data compromise is not equivalent to compromise of a name and address, and a notification that obscures the distinction is not an adequate notification.

22.3 Cooperation

Bioprium will cooperate fully with the Hospital's investigation and notification, **mitigate any known harmful effect of an impermissible use or disclosure** — an obligation Bioprium assumes by contract in the Business Associate Agreement, mirroring the duty the Privacy Rule places on covered entities at § 164.530(f) — preserve forensic evidence, and make personnel available. **Bioprium will not delay notification to the Hospital pending completion of its own investigation.**

22.4 To individuals and regulators

Notification of individuals under 45 C.F.R. § 164.404 is the Covered Entity's obligation. Bioprium will support it and, where the Business Associate Agreement so provides and the Hospital elects, will make notifications on the Hospital's behalf at Bioprium's expense where the incident arose from Bioprium's systems.

For Tier Two data, Bioprium will notify affected individuals and regulators directly as applicable state breach notification law requires. Bioprium is not a "vendor of personal health records" and is therefore not subject to the FTC Health Breach Notification Rule, 16 C.F.R. Part 318, for data processed as a Business Associate.

---

23. NOT MEDICAL ADVICE, AND LIMITATIONS OF THE OUTPUT

This section is not conventional privacy-policy content, but it belongs in a document that gates account creation for software of this kind, and it materially reduces the risk of the claims most likely to be brought against you.

23.1 Bioprium does not practice medicine

Bioprium's outputs are **computational predictions and analytical results**. They are not diagnoses, not treatment recommendations, not clinical laboratory results, and not medical advice. They are intended for use by qualified professionals — clinicians, clinical geneticists, genetic counselors, and researchers — who exercise independent professional judgment.

Bioprium is not CLIA-certified. Outputs must not be used as clinical laboratory results or reported as such.

23.2 Regulatory status

Bioprium is designed to function as **Clinical Decision Support software** that discloses its basis so that a healthcare professional can independently review it and does not rely primarily on its recommendations — the criteria distinguishing non-device CDS under section 520(o)(1)(E) of the Federal Food, Drug, and Cosmetic Act, as amended by section 3060 of the 21st Century Cures Act, and FDA's Clinical Decision Support Software guidance.

The provenance and traceability architecture in Section 5.4 exists substantially for this reason. **Bioprium's outputs are not FDA-cleared or FDA-approved**, and Bioprium makes no representation that its software is or is not a medical device in any particular use. A Hospital deploying the Service in a manner that causes a clinician to rely primarily on its output, or that obscures the basis of the output, may change that analysis — and that deployment decision is the Hospital's.

23.3 Known and disclosed limitations

Every dossier the Service generates carries a mandatory limitations section, automatically generated from what actually occurred in that run, that cannot be empty and cannot be suppressed. Software behavior that materially bears on interpretation:

- Where two resolving genotype callers contradict one another, the Service reports **indeterminate** and blocks rather than selecting a winner. **Where only one caller resolves a given gene, the Service reports the result together with an explicit single-caller status**, so that a reviewer sees that corroboration was not achieved. Whether a second resolving caller is required is a per-deployment configuration, and Bioprium will state the setting in force for a Hospital's deployment.
- Where no candidate guide meets the selectivity threshold, the Service **refuses to return one** rather than lowering the threshold. "No acceptable guide found" is a result, not a failure.
- Where a required empirical scoring resource is not loaded, the Service **raises an error** rather than substituting an approximation. A fabricated constant produces a confident, wrong ranking that nothing downstream would catch.
- Where quality control fails on the short-read immunogenetics path — insufficient coverage, contamination above threshold, reference mismatch — the Service **halts** rather than proceeding with a caveat. **The long-read repeat-expansion path does not currently run this gate**; extending it is a condition precedent to accepting patient data through that path.
- Analyses whose modules did not run are recorded as explicit **not-run records** naming the reason, rather than being omitted.
- Computational results are described as **"predicted."** The word **"validated"** is reserved for wet-lab-confirmed results, and this is enforced programmatically on rendered output.
- Population-scale validation data does not exist for every locus and range the Service can analyze. Where it does not, the Service says so rather than implying a confidence it has not measured.

These behaviors are deliberate and Hospitals should not request their removal. A vendor who will lower a safety threshold on request is a vendor whose thresholds mean nothing.

23.4 Human review is required

No Bioprium output may be used to make a clinical decision without independent review by a qualified professional. The Service does not make autonomous decisions, does not act without a human in the loop, and is not designed or validated for autonomous use. The Hospital is responsible for ensuring competent human review of every output it acts on.

24. DISCLAIMERS, LIMITATION OF LIABILITY, AND INDEMNIFICATION

Capitalized terms not defined here have the meaning given in the Master Services Agreement between Bioprium and the Hospital. ***Where this policy conflicts with a signed Master Services Agreement or Business Associate Agreement, the signed agreement controls.***

24.1 Disclaimer of warranties

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE SERVICE AND ALL OUTPUTS ARE PROVIDED "AS IS" AND "AS AVAILABLE," WITHOUT WARRANTY OF ANY KIND, EXPRESS, IMPLIED, OR STATUTORY. BIOPRIUM SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, ACCURACY, AND ANY WARRANTY ARISING FROM COURSE OF DEALING OR USAGE OF TRADE.

WITHOUT LIMITING THE FOREGOING, BIOPRIUM DOES NOT WARRANT THAT: THE SERVICE WILL BE UNINTERRUPTED, TIMELY, SECURE, OR ERROR-FREE; ANY OUTPUT WILL BE ACCURATE, COMPLETE, OR CLINICALLY VALID; ANY GUIDE RNA WILL PERFORM AS PREDICTED IN VITRO OR IN VIVO; ANY OFF-TARGET ANALYSIS WILL IDENTIFY ALL OFF-TARGET SITES; ANY GENOTYPE CALL WILL BE CORRECT; OR THAT USE OF THE SERVICE WILL ACHIEVE ANY PARTICULAR RESULT.

COMPUTATIONAL OFF-TARGET PREDICTION IS AN INHERENTLY INCOMPLETE METHOD. THE ABSENCE OF A PREDICTED OFF-TARGET SITE IS NOT EVIDENCE THAT NO OFF-TARGET SITE EXISTS. WET-LAB CONFIRMATION IS REQUIRED BEFORE ANY THERAPEUTIC APPLICATION.

24.2 Allocation of responsibility

The Hospital is solely responsible for:

(a) Obtaining and maintaining all patient consents and authorizations (Section 6);

(b) The lawfulness of every instruction it gives Bioprium;

(c) The accuracy, completeness, quality, and provenance of the Hospital Data it submits;

(d) All clinical interpretation of, and all clinical decisions made in reliance on, any output;

(e) Independent professional review of every output before clinical use (Section 23.4);

(f) Wet-lab validation before therapeutic application;

(g) Compliance with all laws applicable to it as a Covered Entity, healthcare provider, research institution, or employer, including HIPAA, the Common Rule, state genetic privacy law, state medical-records law, professional licensing requirements, and applicable foreign law;

(h) Provisioning, review, deprovisioning, and conduct of its own users;

(i) Security of its own systems, networks, credentials, and endpoints;

(j) Any determination that Bioprium's outputs are suitable for its intended use;

(k) Its own IRB approvals, data use agreements, and research compliance;

(l) Notification of patients following a breach, as the Covered Entity.

Bioprium is not responsible for, and expressly disclaims liability for:

(a) Any consequence of the Hospital's failure to obtain adequate consent or authorization;

(b) Any clinical decision, diagnosis, treatment, or outcome;

(c) Any adverse event, patient injury, or death arising from use of an output;

(d) Any error, defect, or omission in Hospital Data as submitted;

(e) Any use of the Service outside its documented purpose or contrary to its documented limitations;

(f) Any consequence of the Hospital overriding, suppressing, or circumventing a quality-control gate, a refusal, or a threshold;

(g) Any act or omission of the Hospital's personnel, contractors, or other vendors;

(h) Any unauthorized access resulting from compromise of the Hospital's credentials or systems;

(i) Any interpretation of an output by a person who is not a qualified professional;

(j) Any disclosure of a patient's genetic information by the Hospital to any third party;

(k) Any discrimination in insurance, employment, or otherwise arising from a patient learning their genetic status;

(l) Any consequence of a patient learning information they preferred not to know, where the Hospital's consent process did not address the right not to know.

24.3 Limitation of liability

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL BIOPRIUM OR ITS OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, OR LICENSORS BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, EXEMPLARY, OR PUNITIVE DAMAGES, OR FOR ANY LOSS OF PROFITS, REVENUE, DATA, GOODWILL, OR BUSINESS OPPORTUNITY, ARISING OUT OF OR RELATING TO THE SERVICE, WHETHER IN CONTRACT, TORT, STRICT LIABILITY, OR OTHERWISE, AND WHETHER OR NOT BIOPRIUM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

BIOPRIUM'S TOTAL AGGREGATE LIABILITY ARISING OUT OF OR RELATING TO THE SERVICE WILL NOT EXCEED THE GREATER OF (i) THE FEES PAID BY THE HOSPITAL TO BIOPRIUM IN THE TWELVE MONTHS IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO THE CLAIM, OR (ii) [US$ AMOUNT].

Exclusions from the cap. The limitation above does not apply to: Bioprium's indemnification obligations for third-party intellectual property claims; Bioprium's gross negligence, willful misconduct, or fraud; Bioprium's breach of its confidentiality obligations; **or liability that cannot be limited or excluded as a matter of law.**

A note on the security carve-out. Hospital counsel will ordinarily require that liability for a security breach caused by Bioprium's failure to meet its security obligations be subject to a **super-cap** — commonly a multiple of annual fees — rather than the general cap.

Jurisdictional limits. Some jurisdictions do not allow the exclusion of implied warranties or the limitation of liability for certain damages. In those jurisdictions, the exclusions and limitations above apply to the maximum extent permitted, and nothing here excludes liability for death or personal injury caused by negligence, for fraud, or for any other liability that cannot lawfully be excluded.

24.4 Indemnification by the Hospital

The Hospital shall indemnify, defend, and hold harmless Bioprium and its officers, directors, employees, agents, successors, and assigns from and against all claims, liabilities, losses, damages, fines, penalties, judgments, settlements, and expenses (including reasonable attorneys' fees and costs of investigation) arising out of or relating to:

(a) Any breach of the representations and warranties in Section 6.2;

(b) Any failure to obtain, maintain, or honor patient consent or authorization;

(c) Any claim by a patient, a patient's family member, a patient's estate, or a class thereof relating to the collection, use, or disclosure of data the Hospital submitted;

(d) Any clinical decision made in reliance on an output;

(e) Any adverse event, injury, or death arising from a therapeutic application;

(f) Any breach of the Hospital's obligations under HIPAA, state genetic privacy law, the Common Rule, or any other law applicable to the Hospital;

(g) Any unauthorized access resulting from compromise of the Hospital's credentials, systems, or personnel;

(h) Any submission of data the Hospital was not authorized to submit, including data subject to 42 C.F.R. Part 2 submitted without notice;

(i) Any use of the Service outside its documented purpose or contrary to its documented limitations.

Except to the extent the claim arises from Bioprium's own gross negligence, willful misconduct, fraud, or breach of its obligations under Section 17.

24.5 Indemnification by Bioprium

Bioprium shall indemnify, defend, and hold harmless the Hospital against claims that the Service, as provided by Bioprium and used in accordance with its documentation, infringes a third party's United States patent, copyright, trademark, or trade secret.

24.6 Basis of the bargain

The Hospital acknowledges that the disclaimers, allocations, and limitations in this Section 24 reflect a reasonable allocation of risk between commercially sophisticated parties, are a material inducement to Bioprium's provision of the Service at the agreed pricing, and form an essential basis of the bargain. **These provisions apply even if a limited remedy is found to have failed of its essential purpose.**

---

25. GOVERNING LAW AND DISPUTES

This policy is governed by the laws of **[STATE]**, without regard to conflict of laws principles. Venue for any dispute lies in [COUNTY, STATE]. [STATE YOUR ARBITRATION AND CLASS-ACTION-WAIVER TERMS, OR DELETE THIS SENTENCE].

Nothing in this section limits any right a patient or consumer has to file a complaint with the HHS Office for Civil Rights, a state attorney general, a state privacy regulator, or a data protection supervisory authority.

---

26. CHANGES TO THIS POLICY

We may update this policy. When we do:

- The **Effective Date** and **Version** at the top are updated.

- **Material changes** — a new category of data collected, a new purpose, a new category of recipient, a change to secondary-use rights, or a reduction in your rights — are notified to account holders by email and by prominent notice on the website at least **[30] days** before taking effect.
- **Material changes affecting Hospital Data** are notified to each Hospital at least **[30] days** in advance, and a Hospital that objects may terminate without penalty and require deletion.
- **We do not apply material changes retroactively to data already collected** without a lawful basis for doing so, and where consent was the basis we obtain fresh consent.
- A **change log**, with prior versions, is maintained at **[URL]**. Prior versions remain available so you can see exactly what changed and when.

Continued use after the effective date of a change constitutes acceptance of the updated policy for Tier Two data. For Hospital Data, the Business Associate Agreement and Master Services Agreement govern and are amended by their own terms.

---

27. CONTACT

Privacy questions and rights requests: **privacy@[DOMAIN]** Security vulnerability disclosure: **security@[DOMAIN]** (PGP key at [URL]) HIPAA Privacy Official: **[NAME, TITLE, EMAIL]** HIPAA Security Official: **[NAME, TITLE, EMAIL]** Data Protection Officer (EU/UK): **[NAME / "not appointed"]** EU / UK representative under Article 27: **[NAME AND ADDRESS]** Post: [LEGAL ENTITY NAME], [ADDRESS] Telephone: **[TOLL-FREE NUMBER]**

To file a complaint:

- **HHS Office for Civil Rights** — https://www.hhs.gov/ocr/complaints — 1-800-368-1019
- **Your state attorney general**
- **California Privacy Protection Agency** — https://cppa.ca.gov
- **Your EU/UK supervisory authority**, where applicable

We will not retaliate against anyone for filing a complaint or exercising a right.

APPENDIX A — SUMMARY OF WHO IS RESPONSIBLE FOR WHAT

The Hospital is responsible for:

- Obtaining patient consent and authorization
- Verifying that the scope of that consent covers processing by a third-party vendor
- Obtaining IRB approval where the processing constitutes research
- Providing its Notice of Privacy Practices to patients
- Applying the minimum necessary standard before submitting data
- Choosing pseudonymous sample identifiers
- Holding the re-identification key
- Determining which state genetic privacy law applies to a given patient
- Clinical interpretation of every output
- Independent professional review before any clinical use

- Wet-lab validation before any therapeutic application
- Genetic counseling and delivery of results to patients
- Provisioning, reviewing, and deprovisioning its own users
- Notifying patients following a breach, as the Covered Entity

Bioprium is responsible for:

- Securing data within Bioprium's environment
- Encryption in transit and at rest
- Access controls and audit logging
- Subprocessor due diligence and Business Associate Agreements
- Breach notification to the Hospital
- Honoring deletion instructions
- Keeping patient-derived sequence off third-party services
- Deleting whole-genome source files once a slice is produced
- Provenance and traceability of outputs
- Refusing to degrade safety thresholds on request
- Its own direct HIPAA compliance as a Business Associate

Shared, with the Hospital leading and Bioprium supporting: responding to patient access and amendment requests, notifying patients after a breach, and managing Hospital user access, for which Bioprium supplies the tooling and the Hospital makes the decisions.

APPENDIX B — DOCUMENT HIERARCHY

Where documents conflict, the following order controls:

1. **Business Associate Agreement** — governs all PHI
2. **Master Services Agreement** and any Data Processing Addendum
3. **Order Form** or Statement of Work
4. **This Privacy Policy**
5. **Terms of Service**
6. Product documentation

This Privacy Policy is a notice document. It is not a substitute for a Business Associate Agreement, and no Hospital should submit PHI in reliance on it alone.

Bioprium — [LEGAL ENTITY NAME]. Version 1.0, effective [DATE].
