

Exelixis, Inc. Notice of Privacy Practices—Self-Funded Plans

Effective Date: November 1, 2022

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

Exelixis, Inc. (“Exelixis”) offers various health care options to its employees and retirees, and their eligible family members, through its Welfare Benefits Program. Several options are self-funded group health plans for which Exelixis acts as its own insurer and directly pays the claims. This notice describes the privacy practices that Exelixis has established for these options, which are referred to as the “Self-Funded Plans” or “Plans.” They are managed for Exelixis by Business Associates, which are third-party administrators that interact with the healthcare providers and handle members’ claims (and as further defined below).

The Self-Funded Plans as of the effective date of this notice include BlueShield of California (PPO, PPO-HDHP, EPO), Guardian Dental, VSP Vision, Naiva FSA and Forma HRA.

EXELIXIS’ COMMITMENT

Exelixis is committed to protecting the privacy of your protected health information or PHI. PHI refers to health information that a Self-Funded Plan creates or receives that relates to your physical or mental health, your health care or payment for your health care. In most cases, your PHI is maintained by the business associate that serves as the third-party administrator for the Self-Funded Plan in which you participate, but Exelixis may also hold certain health-related information. Generally, the Exelixis-held information is limited to enrollment data, but in limited instances, it may include information you provide to designated Exelixis staff to help with coordination of benefits (including payment of claims) or resolving complaints.

The privacy protections described in this notice reflect the requirements of federal regulations issued under the Health Insurance Portability and Accountability Act (“HIPAA”). They require the Self-Funded Plans to:

- comply with HIPAA privacy standards and other federal laws;
- make sure that your PHI is protected;
- give you this notice of the Self-Funded Plans’ legal duties and privacy practices with respect to your PHI; and
- follow the terms of the notice that are currently in effect.

HOW THE SELF-FUNDED PLANS WILL USE AND DISCLOSE YOUR PROTECTED HEALTH INFORMATION

The following sections describe different ways that a Self-Funded Plan may use and disclose your PHI. Not every use or disclosure will be listed. All of the ways that a Self-Funded Plan is permitted to use and disclose PHI, however, will fall within

one of the categories. Use and disclosure of some PHI, such as certain drug and alcohol information, HIV information and mental health information, is further restricted.

- **Treatment.** A Self-Funded Plan may use and disclose your PHI in order to assist your health care providers (doctors, hospitals, pharmacies and other care personnel who are involved in providing you with medical treatment or services) in your diagnosis and treatment.
- **Payment.** A Self-Funded Plan may use and disclose your PHI to pay claims from doctors, hospital and other providers for services delivered to you that are covered by your plan, to determine your eligibility for benefits, to coordinate benefits, to examine medical necessity, to obtain premiums, or to be reimbursed by another entity that may be responsible for payment.
- **Health Care Operations.** A Self-Funded Plan may use and disclose your PHI in order to perform our plan activities, such as quality assessment activities or administrative activities, including data management or customer service. In some cases, a Self-Funded Plan may use or disclose your information for underwriting purposes, determining premiums, and the detection and investigation of fraud. A Self-Funded may also engage a business associate to carry out health care operations on behalf of the entire Welfare Benefits Program.
- **Plan Sponsor.** A Self-Funded Plan may disclose summary health information (that is, claims data that is stripped of most individual identifiers) to Exelixis in its role as plan sponsor in order to obtain bids for health insurance coverage or to facilitate modifying, amending or terminating such plan. A Self-Funded Plan may also provide Exelixis enrollment or disenrollment information. In addition, if you request help from Exelixis in coordinating your benefits or resolving a complaint, a Self-Funded Plan may disclose your PHI to designated Exelixis staff, but no PHI may be disclosed to facilitate employment-related actions or decisions or for matters involving other benefits or benefit plan. Exelixis may not further disclose any PHI that is disclosed to it in these limited instances.
- **As Required By Law.** A Self-Funded Plan will disclose your PHI if required to do so by federal, state or local law or regulation.
- **Business Associates.** A Self-Funded Plan may disclose PHI to persons or entities that provide services to the Self-Funded Plan so long as the Self-Funded Plan obtains assurances that the Business Associate will comply with HIPAA and the Self-Funded Plan’s procedures on the use and disclosure of PHI.

- **Public Health Activities.** A Self-Funded Plan may disclose your PHI to public health agencies for reasons such as prevention or controlling disease, injury or disability.
- **To Avert a Serious Threat to Health or Safety.** A Self-Funded Plan may disclose your PHI when necessary to prevent or lessen a serious threat to your health and safety or the health and safety of the public or another person. Any disclosure, however, would only be to someone able to help prevent the threat.
- **Research.** In limited circumstances, a Self-Funded Plan may use and disclose PHI for research purposes, subject to the confidentiality provisions of state and federal law. Your PHI may be important to further research efforts and the development of new knowledge. All research projects conducted by Exelixis must be approved through a special review process to protect member safety, welfare and confidentiality.
- **Health Oversight Activities.** A Self-Funded Plan may disclose PHI to governmental, licensing, auditing and accrediting agencies, including, but not limited to state insurance departments and the U.S. Department of Labor, as authorized or required by law.
- **Legal Proceedings.** A Self-Funded Plan may disclose PHI to courts, attorneys and court employees in the course of conservatorship and certain other judicial or administrative proceedings.
- **Lawsuits and Disputes.** If you are involved in a lawsuit or other legal proceeding, a Self-Funded Plan may disclose your PHI in response to a court or administrative order or in response to a subpoena, discovery request, warrant, summons or other lawful process.
- **Law Enforcement.** If authorized or required by law, a Self-Funded Plan may disclose your PHI under limited circumstances to a law enforcement official in response to a warrant or similar process, to identify or locate a suspect or to provide information about the victim of a crime.
- **Additional Uses and Disclosures.** A Self-Funded Plan may also use or disclose your PHI in other ways as permitted by law, including, but not limited to:
 - Specialized government functions, including, but not limited to, military command authorities, national security and intelligence organizations, presidential protective services and correctional institutions;
 - Workers' compensation programs;
 - Coroners, medical examiners and funeral directors;
 - The U.S. Food and Drug Administration; and
 - Organ and tissue donation organizations.

- **With an Authorization.** Other uses and disclosures of your PHI will be made only with your written authorization, unless otherwise permitted or required by law. You may revoke an authorization at any time in writing, except to the extent that the Self-Funded Plan has already taken action on the information disclosed or if the Self-Funded Plan is permitted by law to use the information to contest a claim or coverage under the Plan.

REQUIRED DISCLOSURES

A Self-Funded Plan may be required to disclose your PHI to the U.S. Department of Health and Human Services (HHS) if the Secretary of HHS is conducting a compliance audit.

YOUR RIGHTS

In addition to any rights that may be afforded to you under applicable privacy laws in the jurisdiction where you reside, you also have the following rights under HIPAA regarding the PHI that a Self-Funded Plan maintains about you:

- **Right to Inspect and Copy.** With certain exceptions, you have the right to inspect and obtain a copy of your PHI that is maintained by or for a Self-Funded Plan. Usually the records include enrollment, billing, claims payment and case or medical management records. To inspect and obtain a copy of the PHI, you must submit your request in writing to Exelixis' HIPAA Plan Officer at the email address noted below. You may be charged a fee for the costs of copying, mailing or other supplies associated with your request.

A Self-Funded Plan may deny your request to inspect and/or obtain a copy in certain limited circumstances. For example, HIPAA does not permit you to access or obtain copies of psychotherapy notes. If your request is denied, you will be informed in writing, and you may request that the denial be reviewed. The person conducting the review will not be the person who denied your request. The Self-Funded Plan will comply with the outcome of the review.

- **Right to Request an Amendment.** If you believe that the PHI maintained by a Self-Funded Plan is incorrect or incomplete, you may request that the Plan amend the information. You have the right to request an amendment for as long as the information is kept by or for the Plan. A request for an amendment should be made in writing and submitted to the HIPAA Plan Officer at the email address noted below. In addition, you must provide a reason that supports your request.

A Self-Funded Plan may deny your request for an amendment if it is not in writing or does not include a reason to support the request. In addition, the Plan may deny your request if you ask to amend information that: (i) was not created by the Plan; (ii) is not part of the PHI maintained by or for the Plan; (iii) is not part of the information that you would be permitted to inspect and copy under the law; (iv) is accurate and complete. If the request is denied, the Plan will notify you in writing. You then have a right to submit a written statement of

disagreement with the Plan's decision and the Plan has a right to rebut that statement.

If the request is granted, the Plan will forward your request to other entities that you identify that you want to receive the corrected information. For example, if your PHI has been disclosed to the Exelixis staff so that it may help coordinate benefits or resolve a complaint, you may direct the Plan to share the correction with the designated staff members.

- **Right to an Accounting of Disclosures.** You have the right to receive an accounting of disclosures, which is a list of disclosures such as those that were made of PHI about you, with the exception of certain documents including those relating to treatment, payment and health care operations and disclosures made to you or consistent with your authorization. To request an accounting of disclosures, you must submit your request in writing to the HIPAA Plan Officer at the email address noted below. Your request must state a time period, which may not be longer than six (6) years prior to the date on which the accounting is requested. Your request should indicate in what form you want the list (for example, on paper or electronically). The first list you request within a twelve (12) month period will be free. For additional lists, the Plan may charge you for the cost of providing the list. You will be notified of any costs involved and you may choose to withdraw or modify your request at that time before any costs are incurred.
- **Right to Request Restrictions.** You have the right to request a restriction or limitation on the use and disclosure of your PHI for treatment, payment or health care operations, or to request a restriction on the PHI that the Plan may disclose about you to someone who is involved in your care or the payment for your care, such as a family member or friend. The Plan is not required to agree to your request. If the Plan agrees to your request, it will comply with the requested restriction, unless the information is needed to provide you emergency treatment or to assist in disaster relief efforts. To request a restriction, you must submit your request in writing to the HIPAA Plan Officer at the email address noted below. Your request should state the information you want to limit; whether you want to limit the Plan's use, disclosure or both; and to whom you want the limits to apply, for example, disclosures to your spouse.
- **Right to Request Confidential Communications.** You have the right to request that a Self-Funded Plan communicate with you about medical matters in a certain way or at a certain location. For example, you can ask that the Plan only contact you at work or by mail to a specific address. To request confidential communications, you must submit your request in writing to the HIPAA Plan Officer at the email address noted below. The Plan will accommodate all reasonable requests and will not ask you the reason for your request. Your request must clearly specify how or where you wish to be contacted.

- **Right to a Paper Copy of This Notice.** You may ask Exelixis to give you a copy of this notice at any time. Even if you have agreed to receive this notice electronically, you are still entitled to a paper copy of this notice. To obtain a paper copy of this notice, contact the HIPAA Plan Officer at the email address noted below.
- **Right to Choose Someone to Act for You.** If you have given someone medical power of attorney or if someone is your legal guardian, that person can exercise your rights and make choices about your health information. We will make sure the person has this authority and can act for you before we take any action.
- **Other Uses of Medical Information.** Other uses and disclosures of PHI not covered by this notice will be made only with your written permission. This includes most uses and disclosures of psychotherapy notes, uses and disclosures of PHI for marketing purposes and uses and disclosures of PHI that constitute a sale of PHI. If you provide Exelixis permission to use or disclose your PHI, you may revoke that permission, in writing, at any time. If you revoke your permission, the Plan will no longer use or disclose your PHI for the reasons stated in your written authorization. Please understand that the Plan cannot take back any disclosures already made with your permission.
- **Breach.** You have the right to be notified of the discovery of a breach of unsecured PHI.
- **Genetic Information is Protected Health Information.** In accordance with the Genetic Information Nondiscrimination Act ("GINA"), a Self-Funded Plan will not use or disclose genetic information for underwriting purposes, which includes eligibility determinations, premium computations, applications of any pre-existing condition exclusions and any other activities related to the creation, renewal or replacement of a contract of health insurance or health benefits.

CHANGES TO THIS NOTICE

- The Self-Funded Plans reserve the right to change this notice and to make the revised or changed notice effective for PHI your Plan already maintains on you as well as any information the Plan receives or creates in the future.
- A copy of the current notice will be posted on Exelixis' website at https://nexus.exelixis.com/departments/human_resources/hr_general_resources/hr_forms/benefits/health_benefits/notices/hipaa_privacy_noticedocx. The notice will contain the effective date on the first page, in the top right-hand corner. In addition, a copy of the notice that is currently in effect will be given to new health plan members and will thereafter be available upon request.

COMPLAINTS

If you believe your privacy rights have been violated, you may file a complaint with the carrier, Third Party Administrator, the Self-Funded Plan, and/or with the U.S. Department of Health

and Human Services Office for Civil Rights. All complaints must be made in writing and sent to the address listed below:

U.S. Department of Health and Human Services:

200 Independence Avenue, S.W.

Washington, D.C. 20201,

Telephone: 877-696-6775,

Website: www.hhs.gov/ocr/privacy/hipaa/complaints

You will not be retaliated against for filing a complaint.

QUESTIONS

If you have questions or for further information regarding this privacy notice, contact the HIPAA Plan Officer at hipaa@exelixis.com.

NOTICE INFORMING INDIVIDUALS ABOUT NONDISCRIMINATION AND ACCESSIBILITY REQUIREMENTS

Discrimination is against the law. Exelixis' Self-Funded Plans do not discriminate on the basis of ancestry, race, ethnicity, color, national origin, age, disability or sex/gender (including pregnancy), sexual orientation, gender identity or expression, physical or mental disability, medical condition, veteran status, marital status, genetic information, or on any other basis or characteristic prohibited by applicable federal, state or local law.

Exelixis' Self-Funded Plans:

- Provide free aids and services to people with disabilities to communicate effectively with us, such as:
 - Qualified sign language interpreters
 - Written information in other formats (large print, audio, accessible electronic formats, other formats)
- Provide free language services to people whose primary language is not English, such as:
 - Qualified interpreters
 - Information written in other languages

If you need these services, or if you believe that Exelixis' Self-Funded Plans have failed to provide these services or discriminated in another way, and you need help filing a grievance, please reach out to Exelixis' Benefits team at benefits@exelixis.com

Carrier/ TPA	Filing a Complaint / Questions
BlueShield of California (PPPO, PPO-HDHP, EPO)	Blue Shield of California Privacy Office P.O. Box 272540 Chico, CA 95927-2540 Toll-Free Telephone: 1-888-266-8080 Email Address: blueshieldca_privacy@blueshieldca.com
Guardian Dental	Privacy Policy Link: https://www.guardianlife.com/privacy-policy Customer Response Unit at 800-627-4200 or CRU@glic.com Attention: Guardian Corporate Privacy Officer National Operations The Guardian Life Insurance Company of America Group Quality Assurance - WRO P.O. Box 2457 Spokane, WA 99210-2457
VSP Vision	VSP Attn: Complaint & Grievance Unit PO Box 997100 Sacramento, CA 95899-7100 1-800-877-7195
Navia FSA	Phone: 800-669-FLEX ESteam3@naviabenefits.com
Forma HRA	Privacy Policy Link: https://www.joinforma.com/legal/privacy-policy privacy@joinforma.com and Accounting@joinforma.com

Self-Funded Plan:

Exelixis, Inc.

1851 Harbor Bay Parkway

Alameda, CA 94502

Attn: HIPAA Plan Officer

hipaa@exelixis.com