UNITEDHEALTH GROUP®

EMPLOYEE PERSONAL INFORMATION HANDLING POLICY
U.S. Employees

Introduction

UnitedHealth Group is committed to protecting its workers' personal information.

UnitedHealth Group observes principles of good information handling and takes all reasonable care when handling workers' "Personal Information," which includes any information that identifies, or is capable of identifying, individual UnitedHealth Group employees and other non-employee workers, such as third-party contractors (collectively referred to as "workers"). UnitedHealth Group processes workers' Personal Information in accordance with applicable privacy and data protection laws.

For the purposes of this policy, all UnitedHealth Group subsidiaries and business units are collectively referred to as "UnitedHealth." Any reference to UnitedHealth, "we," "our," "us," or "company" in this policy means UnitedHealth Group and its affiliates.

For information about the privacy rights of California residents, click here.

What Personal Information may we hold about you?

UnitedHealth may collect and use in its day-to-day business activities Personal Information you provided before and during the work relationship. Such information is collected from you and by our company technology and systems when you use them. Personal Information may be obtained from: your application materials including resume or CV; offer letter; any employment contract, independent contractor agreement and/or other professional contract; information used for payroll processing and benefits administration; performance appraisals or disciplinary records; training records; company devices or vehicles; photos used for an identification badge or organizational chart, marketing, or website; biometric data, including biometric data used for timekeeping or facility access; backup files; browsing history or search history (on company-owned or provided devices); internal or external contact information maintained in the onboarding, Human Resources Information System, active directory or other systems; information captured from video or audio systems or other forms of monitoring or surveillance; data collected as part of the company's human capital analytics or talent management programs; occupational health records and assessments, including disease testing results and vaccination records; background checks; drug screenings; payroll service records; and leave and accommodation service records.

How will we use your Personal Information?

UnitedHealth collects Personal Information about you to establish and manage UnitedHealth's relationship with you and for related functions including for personnel and administrative processes (among others) such as, but not limited to:

- To contact you in response to your request or the reason for which you provided your Personal Information to us;
- Human resources administration;
- Carrying out obligations and exercising rights under applicable employment laws;

- Compliance with applicable laws and regulations and UnitedHealth's legal obligations, including accounting and tax requirements and in relation to benefits administration;
- Business processes including maintenance of business and statutory records, management analysis, audits, forecasts, planning, transactions, business continuity, organizational risk management and insurance, and labor risk prevention;
- The security of the workplace, assets, workers and the Personal Information of workers, clients, and customers, including monitoring, as described below;
- Programs and policies on training and development, job evaluation, rewards, planning, and organization;
- The performance of employment and services contracts, including human resource administration and payroll; and
- To manage our occupational health and safety obligations.

UnitedHealth also may screen applicable workers against professional body registrations and licensing organizations. Such screenings are necessary to ensure that workers are suitable for their position at UnitedHealth Group and, in particular, to confirm that they are permitted without exception to provide services to UnitedHealth and all of UnitedHealth's clients, including organizations that prohibit excluded or debarred individuals from working on their account.

Will your Personal Information be kept up to date?

We will only retain Personal Information about you that is necessary for the purposes described above and will take all reasonable steps to ensure that it is kept up-to-date and accurate. From time to time we may ask you to review and update the Personal Information we hold (although you are encouraged to update the information at any time). We will only hold your Personal Information for as long as it is relevant to your working relationship with UnitedHealth or as long as necessary to comply with any legal obligation or to fulfill the above-listed purposes.

In order for us to keep your Personal Information up to date, you must inform us of any changes to the Personal Information we hold about you, for example, your name, address, marital status, contact details, qualifications and emergency contact details.

Do we share your Personal Information with anyone else?

Sometimes we may need to share your Personal Information with third parties. We will only do so when necessary for legitimate business purposes. For example, your Personal Information may be sent to the following parties for the following reasons:

- To external suppliers to administer your benefits on our behalf;
- To clients for the purpose of potentially offering your services to or seconding you to work for them;
- To clients to review your qualifications with a view to securing business;
- To competent public corporations and government authorities as may be required by law regarding tax, labor, social security and similar matters;
- To our carefully selected service providers appointed from time to time to provide services related to our business and under contract to us, such as processors of reimbursable expenses, salary, and other compensation information. Those service providers will be carefully selected and bound by appropriate contractual protections (such as to use appropriate measures to protect the confidentiality and security of personal data), where required by applicable data protection law;

- To internal UnitedHealth business segments that may carry out shared services functions, such as those processing reimbursable expense payments;
- To providers of labor risk prevention and occupational health services;
- To new (or prospective) contractors, if required under transfer of undertakings arrangements;
- To future employers or financial institutions for the purpose of providing a reference/credit references and other information, but only if you request that we do so;
- To any new (or prospective) owners, should there be a change (or prospective change) in the ownership of UnitedHealth, or business units or departments within UnitedHealth in which you work; and/or
- To external parties as required by law or legal process, or as otherwise authorized by you.

State Consumer Privacy Notice

This State Consumer Privacy Notice applies to residents of California and supplements our Employee Personal Information Handling Policy. It explains what Personal Information (PI) we collect about you, where and from whom we obtain it, why we collect it, and your respective rights regarding it. If you are a California resident, this notice applies to any PI that we collect about you.

PI We Collect and Disclose for Business Purposes

In the preceding twelve (12) months, we may have collected the following PI about California residents and have disclosed it for the business purposes described below:

Category of PI	Examples	Collected	Categories of Third Parties to Which We Disclose PI for Business Purposes	Shared for Advertising Purposes	Categories of Third Parties with Which We Share PI for Advertising Purposes
Some Personal Information included in the categories below may overlap with other categories.					
Identifiers	A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, government-issued identification numbers or other similar identifiers.	Yes	Vendors	No	None
Personal information categories	A name, signature,	Yes		No	None

	address, telephone number, government-issued identification numbers, insurance policy number, education, employment, employment history, bank account number, or any other financial information, medical information, or health insurance information.		Vendors		
Protected classification characteristics	Age, race, color, national origin, citizenship, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), veteran or military status.	Yes	Vendors	No	None
Sensitive personal data categories (“Sensitive Personal Data”)	Government-issued identification number, precise geolocation information, contents of an email or text messages, racial or ethnic origin, biometrics data, health data, mental or	Yes	Vendors	No	None

	physical health condition or diagnosis, sexual orientation, citizenship or immigration status.				
Commercial information	Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	No	None	No	None
Biometric information	Fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, or exercise data.	Yes	Vendors	No	None
Internet and/or network activity	Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement.	Yes	Vendors	No	None
Geolocation data	Physical location or movements.	Yes	Vendors	No	None
Sensory data	Audio, electronic, visual, or similar information.	No	None	No	None
Professional or employment-related information	Current or past job history or performance evaluations.	Yes	Vendors	No	None
Education information subject to the Family	Education records directly	Yes		No	None

Educational Rights and Privacy Act	related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, or student disciplinary records.		Vendors		
Inferences drawn from other personal information	Profile reflecting a person's preferences, characteristics, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	No	None	No	None
We will retain the foregoing categories of PI consistent with our internal record-retention policies and for as long as is necessary to provide products and services to you or as required by law.					

PI does not include:

- De-identified or aggregated consumer information
- Publicly available information from government records
- Health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the California Confidentiality of Medical Information Act (CMIA) or clinical trial data
- PI covered by other privacy laws, including: The Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA), the California Financial Information Privacy Act (FIPA), and the Driver's Privacy Protection Act of 1994

Categories of Sources of PI

We obtain the categories of PI listed above from:

- You or your authorized agent,
- Service providers,
- Affiliates,
- Publicly available information,
- Organizations with which you are employed or affiliated, or
- Activity on our apps and websites.

Collection from these sources may occur online, in person, via paper or other electronic means, and may occur automatically where state law permits such profiling absent an explicit request to opt-out.

Why We Collect PI

We collect your PI for one or more of the following business purposes:

- To respond to an email or particular request from you
- To communicate with you
- To personalize services for you
- To process an application as requested by you
- To administer surveys and promotions
- To provide you with information that we believe may be useful to you, such as information about products or services provided by us or other businesses
- To perform analytics and to improve our products, websites, and advertising
- To comply with applicable laws, regulations, and legal processes
- To protect someone's health, safety, or welfare
- To protect our rights, the rights of affiliates or related third parties, or take appropriate legal action
- To keep a record of our transactions and communications
- To detect and protect against security incidents
- To debug to identify and repair errors
- As otherwise necessary or useful for us to conduct our business, so long as such use is permitted by law

Sharing or Selling Your PI

In the preceding twelve (12) months, we have not sold or shared any PI.

Third parties are not allowed to use or disclose your PI other than as specified in our contract and as permitted by law.

If we seek to use your PI for a materially different purpose than we previously disclosed in this notice, we will notify you and will not use your PI for this new purpose without your explicit consent.

Sensitive Personal Data

We only process Sensitive Personal Data to process transactions necessarily related to your employment or application for employment.

How Long We Retain Your PI

We will retain your PI for as long as we provide products and services to you or as required by law.

Your Rights

1. You have the right to request that we disclose certain information to you about our collection and use of your PI over the preceding twelve (12) months prior to your request. Once we receive and confirm your verifiable consumer request, we will disclose to you:

- What PI we collect about you
- Where and from whom we collect PI about you
- Our business purpose for collecting PI about you
- The types of third parties with whom we share your PI
- The specific pieces of PI we collect about you, in a readily-usable format—note that we will not disclose your actual Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, or security questions and answers
- The types of PI that we disclosed about you for a business purpose, and the categories of third parties to whom we disclosed your PI

2. You have the right to be informed about the PI that we collect about you at the time that or before we collect it. This is that notice.

3. You have the right to request that we delete any PI about you that we have.

4. You have the right to request a correction of any inaccurate information in the PI we collect about you.

5. You have the right to stop us from sharing your PI to display advertisements to you based upon your activities, preferences, and interests.

6. If we use your sensitive PI for purposes other than to render services or offer products to you, you will have the right to request that we limit the processing of your sensitive PI.

7. You will not be discriminated against or penalized for exercising your rights to your PI, and we will honor your rights by not:

    - Denying you services,
    - Charging you different prices or rates for services,
    - Imposing penalties, or
    - Providing you with a different level or quality of services.

8. Applicable law may require or permit us to decline your request. If we decline your request, we will tell you why and you may appeal this decision (see additional information in Appeals section below).

How to Exercise Your Rights

- You may exercise your rights by:
    - Calling us at 1-800-561-0861. Let us know you are calling about a "CPRA Request."
    - Submitting a webform here. Include "CPRA Request" in the notes of the webform.
- You may be required to submit proof of your identity for these requests to be processed.
- We will not be able to comply with your request if we are unable to confirm your identity.
- You may designate an authorized agent to make a request on your behalf subject to proof of identity and authorization.

Timing

- Our responses to any of your requests for the information described above will be limited to information that we have collected in the preceding twelve (12) months before our receipt of your verified request.
- We will acknowledge receipt of your request within 10 days of receipt of your submission. You will receive our response to your request within 45 days of your request, unless we provide you with notice that it will take more than 45 days to respond (in that case, we won't take more than 90 days to respond).

Appeals

- If the business denies any of your requests, you may appeal by:
  - Calling us at 1-800-561-0861. Let us know you are calling about a "CPRA Request."
  - Submitting a webform here. Include "CPRA Request" in the notes of the webform.
- We will respond to your appeal within 45 days of receipt, unless we notify you that we will require an additional 15 days to respond.
- If you remain concerned about the result of that appeal, you may contact the attorney general in your state of residency.

What are your obligations under this policy?

We request that you provide us with accurate and up-to-date Personal Information. Should you make a request to access the information we hold about you, we may require that you provide us with further information so that we can be satisfied of your identity, subject to any applicable local restrictions.

Monitoring

To protect UnitedHealth, its assets, workers and the Personal Information of its workers, clients, and customers and to manage and optimize worker performance UnitedHealth performs monitoring and recording activities in the company premises, including offices, workstations, workspaces, other facilities (collectively referred to as "company premises") and company technology and systems, including device location.

UnitedHealth provides workers with access to company premises and its company technology and systems including telephones, fax machines, computers, networks, the Internet and other electronic devices for business and communication purposes.

We permit very limited personal use of company technology and systems, so long as it is in accordance with use policies that are notified to workers. UnitedHealth monitors worker use of company technology and systems for legitimate organizational, compliance, performance, production, and security purposes, including to protect the business of the company and use of its assets and the Personal Information we hold about our clients, customers, and members. All monitoring, which is subject to applicable law, will be proportionate to the potential harm that might be suffered through misuse. If any company technology and systems to which you have access are subject to monitoring, the nature of that monitoring and its purpose will be described to you through company notices and policies.

UNITEDHEALTH GROUP®

What security measures do we employ in handling your Personal Information?

UnitedHealth Group takes appropriate physical, technical and administrative security measures to guard against unauthorized or unlawful access and processing of your Personal Information, and against accidental loss or destruction of, or damage to, your Personal Information, and to ensure that your Personal Information is stored lawfully and securely. Examples of our security measures include:

- Workers who have access to Personal Information are made aware of their obligations to protect that information;
- Personal Information in paper form is kept in filing cabinets that are only accessible by authorized UnitedHealth workers on a need-to-know basis;
- Personal Information comprising occupational health records and assessments are maintained in confidential medical records, separate from personnel records, and only accessible by Enterprise Occupational Health and Safety;
- Personal Information stored electronically is only accessible by authorized personnel; and
- Printed material displaying Personal Information is disposed of securely, for example, by shredding.

Handling Personal Information on Behalf of UnitedHealth

When handling Personal Information on behalf of UnitedHealth, you must only process information that is necessary, adequate, and relevant for legitimate purposes. You must ensure that Personal Information that identifies an individual is only kept for as long as is necessary for the purposes for which it was obtained. If you properly have access to personally identifiable information, you must not disclose any Personal Information to any other UnitedHealth worker, or to any third party except for the purposes of UnitedHealth business and the proper performance of your duties. In accordance with this policy, you must ensure that Personal Information is kept secure and confidential, and at all times comply with UnitedHealth's other policies relating to confidentiality and data security.
All workers who handle Personal Information are required to comply with this policy and any other UnitedHealth policies and procedures prescribing local data security measures. All workers have a duty of confidentiality. Breaches of security and/or confidentiality will be investigated and remedied by UnitedHealth, as appropriate. Any worker handling Personal Information who knowingly or recklessly discloses that information in contravention of our policies or procedures may be subjected to disciplinary action in accordance with local procedures and applicable local law.

Contact Us

Please contact Employee Center at 1-800-561-0861 if you have any questions.

Last Revised

The effective date of this policy is June 30, 2023.

Changes to this Policy

We will review this notice annually and update it from time to time. Any changes will be posted on this page and will become effective as of the date provided under the "Last Revised" section. We encourage you to review this notice periodically to be sure you are aware of those changes.