GeoEngineers Privacy Notice
January 1, 2023

INTRODUCTION

GeoEngineers, Inc. (GeoEngineers) is providing this Privacy Notice to provide information to its employees, job applicants, temporary agency employees, and independent contractors – and other individuals whose Personal Data is collected for business purposes (such as qualified dependents covered on benefits) – regarding how we collect and use your Personal Data in connection with your employment or other relationship with GeoEngineers. In this Notice, "Personal Data" means data relating to identified or identifiable individuals and households.

SCOPE OF THIS POLICY

This Privacy Notice applies to Personal Data processed in the context of employment and other internal business functions relating to our employees/applicants and their family members or beneficiaries, including internal computer systems, networks, online services, benefits, etc.

This Privacy Notice describes how GeoEngineers collects, uses, and protect the Personal Data of individuals who use the GeoEngineers website and other online services, including our applicant tracking system.

HOW TO CONTACT US

GeoEngineers
17425 NE Union Hill Rd, Ste 250
DataRequest@geoengineers.com
(425) 861-6000

See below for information relating to how to submit requests to exercise your rights in the Personal Data we process.

CATEGORIES OF PERSONAL DATA

This chart describes the categories of Personal Data that GeoEngineers may collect in connection with its employment and contractual work relationships. Note, all Personal Data may be used and disclosed in connection with our Business Purposes.

Category of Personal Data & Representative Data Elements	**Common Purposes for Collecting & Sharing**
Contact Data • Honorifics and titles, preferred form of address • Mailing address • Email address • Telephone number	We use your Contact Data to communicate with you by mail, email, telephone, or text about your application or employment, including sending you scheduling information, compensation and benefits communications (including enrollment with third-party platforms), and other company information.

Category of Personal Data & Representative Data Elements	Common Purposes for Collecting & Sharing
• Mobile number	Contact Data is also used to help us identify you and personalize our communications, such as by using your preferred name.
Identity Data • Full name, nicknames or previous names (such as maiden names) • Date of birth • Language • Employee ID number • Company account identifiers and passwords • Benefits program identifiers • System identifiers (e.g., usernames or online credentials)	We use your Identity Data to identify you in our records and systems, to communicate with you (often using your Contact Data) and to facilitate our relationship with you, for internal record-keeping and reporting (including for data matching and analytics), and to track your use of company programs and assets, for benefits enrollment, and for most processing purposes described in this Privacy Notice, including governmental reporting, employment/immigration verification, background checks, etc.
Government ID Data • Social security/national insurance number • Driver's license information • Passport information • Other government-issued identifiers as may be needed for risk management or compliance (*e.g., if you are a licensed professional, we will collect your license number)*	We use your Government ID Data to identify you and to maintain the integrity of our HR records, enable employment verification and background screening, such as reference checks, license verifications, and criminal records checks (subject to applicable law), enable us to administer payroll and benefits programs and comply with applicable laws (such as reporting compensation to government agencies as required by law), as well as for security and risk management (such as collecting driver's license data for employees who operate company vehicles, professional license verification, fraud prevention and similar purposes). We may also use Government ID data for other customer business purposes, such as collecting passport data and secure flight information for employees and contractors who travel as part of their job duties.
Biographical Data	We use Biographical Data to help us understand our applicants, employees, and contractors and for professional and personal development, to assess suitability for job roles, and to ensure a good fit between each individual's background and relevant job functions.

Category of Personal Data & Representative Data Elements	Common Purposes for Collecting & Sharing
• Resume or CV • Application and screening questionnaires • Data from information publicly available on the Internet • Education and degree information • Employment or other work history • Professional licenses, certifications, and memberships and affiliations • Personal and professional skills and talents summaries (e.g., languages spoken, CPR certification status, community service participation), interests and hobbies • Professional goals and interests • Criminal records	We also use Biographical Data to foster a creative, diverse workforce, for recruiting, for coaching, and to guide our decisions about internal programs and service offerings.
Transaction and Interaction Data • Dates of Employment • Re-employment eligibility • Position, Title, Reporting Information • Work history information • Time and attendance records • Leave and absence records • Salary/Payroll records • Benefit plan records • Housing records • Travel and expense records • Training plan records • Performance records and reviews • Disciplinary records	We use Transaction and Interaction Data as needed to manage the employment relationship and fulfill standard business functions, such as scheduling work, providing payroll and benefits and managing the workplace (e.g., onboarding, maintenance, evaluations, performance management, investigations, etc.).
Financial Data • Bank account number and details • Company-issued payment card information, including transaction records • Tax-related information	We use your Financial Data to facilitate compensation, (such as for direct deposits), expense reimbursement, to process financial transactions, for tax withholding purposes, and for security and fraud prevention.

Category of Personal Data & Representative Data Elements	Common Purposes for Collecting & Sharing
Health Data • Medical information for accommodation of disabilities • Medical information for leave and absence management, and emergency preparedness programs • COVID-19 testing and vaccination data and exposure to COVID-19 • Vaccination status • Wellness program participation • Information pertaining to enrollment and utilization of health and disability insurance programs	We use your Health Data as needed to provide health and well-being programs, including health insurance programs, and for internal risk management and analytics related to our HR functions, staffing needs, and other Business Purposes. In response to the COVID-19 pandemic, we implemented health and other screening procedures, vaccination requirements, vaccination tracking, and other measures to reduce the possibility of transmission to our employees and guests and to comply with applicable public health orders and guidance. While vaccination and testing requirements are no longer a requirement of workplace access (except in cases where required by clients), we continue to store this information. In addition, we use and may need to share COVID-19 infection data to carry out contact tracing, implement and enforce workplace safety rules, and for public safety reasons and compliance obligations.
Device/Network Data • Device information from devices that connect to our networks • System logs, including access logs and records of access attempts • Records from access control devices, such as badge readers • Information regarding use of IT systems and Internet search and browsing history, metadata and other technically-generated data • Records from technology monitoring programs, including suspicious activity alerts • Data relating to the use of communications systems and the content of those communications	We use Device/Network Data for system operation and administration, technology and asset management, information security incident detection, assessment, and mitigation and other cybersecurity purposes. We may also use this information to evaluate compliance with company policies. Our service providers may use this information to operate systems and services on our behalf, and in connection with service analysis, improvement, or other similar purposes related to our business functions.
Inference Data • Performance reviews	We use Inference Data to help tailor professional development programs and to determine suitability for

Category of Personal Data & Representative Data Elements	Common Purposes for Collecting & Sharing
• Results of cybersecurity tests or assigned training.	advancement or other positions. We may also analyze and aggregate data for workforce planning. Certain Inference Data may be collected in connection with information security functions (e.g., patterns of usage and cybersecurity risk).
Compliance and Demographic data • Employment eligibility verification records, background screening records, and other records maintained to demonstrate compliance with applicable laws, such as payroll tax laws, ADA, FMLA, ERISA, etc. • Occupational safety records and workers' compensation program records • Records relating to internal investigations • Records of privacy and security incidents involving HR records, including any security breach notifications	We use Compliance and Demographic Data for internal governance, corporate ethics programs, institutional risk management, reporting, demonstrating compliance and accountability externally, and as needed for litigation and defense of claims.
Protected Category Data Characteristics of protected classifications under state or federal law, e.g. race, national origin, religion, gender, disability, marital status, sexual orientation, or gender identity	We use Protected Category Data as needed to facilitate the employment relationship or other relationship, for compliance and legal reporting obligations, to evaluate the diversity of our applicants/employees and the success of our diversity and inclusion efforts, and as needed for litigation and defense of claims.
Sensitive Personal Data The following categories of data we collect are considered "Sensitive Personal Data:" • Protected Category Data; • Health Data • Financial Data • Government ID	We use Sensitive Personal Data only as strictly necessary for the purpose it is collected with your knowledge and consent if required by law (e.g. health information on a health insurance benefits application, COVID-19 vaccination status for staffing or entry into locations where vaccination is required, and requests for accommodation).

Category of Personal Data & Representative Data Elements	Common Purposes for Collecting & Sharing
• any other Personal Data revealing: • (i) Social security, driver's license, state identification card, or passport number; (ii) company account log-in and password; (iii) racial or ethnic origin; (iv) mailing address and personal email	

SOURCES OF PERSONAL DATA

We collect Personal Data from various sources, which vary depending on the context in which we process that Personal Data.

- **Data you provide us** – We will receive your Personal Data when you provide them to us, when you apply for a job, complete forms, enroll in benefits, or otherwise provide direct information to us.
- **Data from a third party** – We will receive your Personal Data from third parties such as employment screening providers.
- **Data from publicly available sources** – We may collect data that is publicly available on the Internet (e.g. through a Linked In or Google search of a candidate's name).
- **Data we collect automatically** – We may also collect information about or generated by any device you have used to access internal IT services, applications, and networks.
- **Data we receive from Service Providers** – We receive information from service providers performing services on our behalf.
- **Data we create or infer** – We (or third parties operating on our behalf) create and infer Personal Data such as Inference Data based on our observations or analysis of other Personal Data processed under this Privacy Notice, and we may correlate this data with other data we process about you. We may combine Personal Data about you that we receive from you and from third parties.

DISCLOSURE OF PERSONAL DATA

We generally process Personal Data internally; however, it may be shared or processed externally by third party service providers, when required by law or necessary to complete a transaction, or in other circumstances described below.

CATEGORIES OF INTERNAL RECIPIENTS

The Personal Data identified below collected from applicants/employees may be disclosed to the following categories of recipients in relevant contexts.

- **HR Department** – All Personal Data relating to HR and Recruiting.

- **Finance Department** – Personal Data to the extent related to payroll, compensation, expense reimbursements, etc.
- **Managers –** Elements of Personal Data to the extent permitted in the jurisdiction, to the extent necessary to evaluate, establish, and maintain the employment or contractual relationship, conduct reviews, handle compliance obligations, and similar matters.
- **Managers searching for new employees or contractors** – Personal data of job candidates contained in job applications to the extent allowed by relevant laws and departmental needs.
- **IT Administrators** of GeoEngineers and/or third parties who support the management and administration of HR and Finance processes may receive Personal Data as necessary for providing relevant IT related support services (for example, conducting IT security measures and IT support services)**.**
- **Peers and colleagues –** Elements of Personal Data in connection with intracompany and interpersonal communications and other contexts relevant to the day-to-day operation of company business.

CATEGORIES OF EXTERNAL RECIPIENTS

GeoEngineers may provide Personal Data to external third parties as described below. The specific information disclosed may vary depending on context but will be limited to the extent reasonably appropriate given the purpose of processing and the reasonable requirements of the third party and GeoEngineers. We generally provide information to:

- Service providers, vendors, and similar data processors that process Personal Data on GeoEngineers' behalf (e.g., analytics companies, financial analysis/budgeting, trainings, benefits administration, payroll administration, background checks, etc.) or that provide other services for our employees or for GeoEngineers.
- To prospective seller or buyer of such business or assets in the event [COMPANY] sells or buys any business or assets.
- To your employment references, in order to inform them that you have applied with GeoEngineers as part of our recruiting process.
- To future prospective employers seeking to confirm your relationship with GeoEngineers.
- To government agencies or departments, or similar parties in connection with employment related matters.
- To financial institutions or housing owners/property management in the event the employee has provided written permission for GeoEngineers to disclose employment and salary information related to bank loans or housing rentals.
- To any public authority in relation to national security or law enforcement requests, if GeoEngineers is required to disclose Personal Data in response to lawful requests by a public authority.
- To any other appropriate third party, if GeoEngineers is under a duty to disclose or share your Personal Data in order to comply with any legal obligation or to protect the rights,

property, health, or safety of GeoEngineers, our employees, contractors, clients, or others.

Locations of Recipients

GeoEngineers is located in the United States. Any Personal Data collected under this Policy will likely be processed in the United States, in addition to any other jurisdiction where third-party service providers are located.

PURPOSES FOR COLLECTING, USING, AND DISCLOSING PERSONAL DATA

GeoEngineers collects Personal Data about its prospective, current, and former Personnel and other individuals as appropriate in the context of an employment or contractual work relationship (such as dependents) for various general HR and business purposes, as described below. GeoEngineers does not sell or share Personal Data with third parties in exchange for monetary consideration or for advertising purposes.

GENERAL HR PURPOSES

GeoEngineers collects Personal Data about its prospective, current, and former employees, job applicants, contractors and other individuals as appropriate in the context of an employment or contractual work relationship, including for recruitment and IT/technical support services, and as needed for using internal software, networks and devices. The categories of Personal Data we process, along with representative data elements, are listed in the chart below. We may not collect from you or process all of the Personal Data identified below, depending on your position or the nature of your relationship with GeoEngineers.

We generally process Personal Data for the following purposes:

Personal Data pertaining to ***prospective*** employees or contractors may processed for:	• Recruitment and staffing, including evaluation of skills and job placement. • Hiring decisions, including negotiation of compensation, benefits, relocation packages, etc. • Risk management, including reference and other background checks. • Our Business Purposes (defined below).
Personal Data pertaining to ***current*** employees and contractors may be processed for:	• Staffing and job placement, including scheduling and absence management. • Verification of eligibility to work and compliance with immigration laws, rules and regulations. • Administration of compensation, insurance and benefits programs.

	• Time and attendance tracking, expense reimbursement, other workplace administration and facilitating relationships within GeoEngineers. • Technology support uses, such as managing our computers and other assets, providing email and other tools to our workers. • EEO/Affirmative Action programs. • Internal and external directories of employees. • Health and well-being programs. • Reasonable accommodations. • Occupational health and safety programs (including drug and alcohol testing, required injury and illness reporting, disaster recovery and business continuity planning, and workers' compensation management). • Health and safety requirements imposed by GeoEngineers, government authorities, or others, depending on the location of employment, engagement or travel (e.g. vaccination status or health screening). • Talent and performance development, skills management and training, performance reviews, employee feedback surveys, and recognition and reward programs. • HR support services, such as responding to inquiries, providing information and assistance. • Employee relations, such as implementing and administering HR policies, investigations, and resolving disputes or concerns that you may raise. • Risk management and loss prevention, including employee and premises monitoring. • Implementing an effective sickness absence management system including monitoring the amount of leave and subsequent actions to be taken, such as making adjustments. • Managing statutory leave programs such as medical and family leave. • Succession planning and adjustments for restructuring. • As requested by individuals, including to verify employment and income verifications (e.g., for mortgage applications). • Business Purposes (defined below).
Personal Data pertaining to ***former*** employees and contractors may be processed for:	• Re-employment. • Administration of compensation, insurance and benefits programs. • Expense reimbursements. • For archival and recordkeeping purposes.

	• Responding to claims for unemployment benefits and other government inquiries. • As requested by individuals, including employment and income verifications (e.g., for mortgage applications). • EEO/Affirmative Action programs. • Business Purposes (defined below).
Personal Data pertaining to individuals whose information is provided to GeoEngineers in the course of HR management (such as information pertaining to employees' family members, beneficiaries, dependents, emergency contacts, etc.) may be processed for:	• Administration of compensation, insurance and benefit programs. • Workplace administration. • To comply with child support orders or garnishments. • To maintain emergency contact lists and similar records. • Business Purposes (defined below).

BUSINESS PURPOSES

"Business Purposes" means the following purposes for which Personal Data may be collected, used and shared:

- Maintaining comprehensive and up-to-date applicant/employee records.
- Establishing, managing, or terminating the employment or other working relationship.
- Maintaining a safe and respectful workplace and improving employee satisfaction and performance.
- Identity and credential management, including identity verification and authentication, issuing badges/keys, system administration and management of access credentials.
- Security, safety, loss prevention, information security, and cybersecurity.
- Legal and regulatory compliance, including without limitation all uses and disclosures of Personal Data that are required by court orders and applicable laws, regulations, orders and ordinances, and for compliance with legally-mandated policies and procedures, such as anti-money laundering programs, security and incident response programs, intellectual property protection programs, and corporate ethics reporting system, and other processing in connection with the establishment and defense of legal claims.
- Corporate audit, analysis, and consolidated reporting.
- To enforce our contracts and to protect GeoEngineers, our workers, our clients and their employees and the public against injury, theft, legal liability, fraud or abuse, to people or property.
- As needed to de-identify the data or create aggregated datasets, such as for consolidating reporting, research, or analytics.

- Making back-up copies for business continuity and disaster recovery purposes, and other IT support, debugging, security, and operations.
- For the operations, analysis, upgrade, enhancement, development, or improvement internal IT or other services, operations, and similar matters.
- To ship items to an employee's home as needed for day-to-day business operations (e.g., shipping work-related items to remote employees, such as IT equipment, onboarding items, project-related items and resources essential for the employee fulfilling job duties, etc.) Only those GeoEngineers employees whose job duties include responsibility for those business operations items will have access to employee addresses.
- GeoEngineers will only ship non-business-essential items (e.g., company gifts, Company Store orders, etc.) to an employee's home when the employee provides their preferred shipping address directly to the GeoEngineers employee(s) or third party responsible for shipping and when the employee has the option to ship non-business-essential items to a GeoEngineers office instead of to their home. GeoEngineers employees who obtain addresses of other employees for the purpose of shipping non-business-essential items may not retain these addresses once shipment is complete.
- As needed to facilitate corporate governance.

DATA ADMINISTRATION

SECURITY

GeoEngineers requires that Personal Data be protected using technical, administrative, and physical safeguards, as described in our various security policies. GeoEngineers' staff must follow the security procedures set out in applicable security policies at all times.

RETENTION AND DISPOSAL

GeoEngineers intends to retain Personal Data or Sensitive Personal Data (as defined above) for no longer than is reasonably necessary and proportionate to achieve the legitimate business purpose for which it was collected or to satisfy a legal requirement. What is necessary may vary depending on the context and purpose of processing. We generally consider the following factors when we determine how long to retain data (without limitation):

- Retention periods established or necessary under applicable law;
- Industry and human resources best practices;
- Whether the purpose of processing is reasonably likely to justify further processing;
- Risks to individual privacy in continued processing;
- Applicable data protection impact assessments;
- IT systems design considerations/limitations; and
- The costs associated continued processing, retention, and deletion.

GeoEngineers staff must follow any applicable records retention schedules and policies and destroy any media containing Personal Data or Sensitive Personal Data in accordance with applicable company policies. Personal Data shall not be further processed in a manner that is incompatible with these purposes.

We retain certain Personal Data for specific periods, as follows:

Category of Personal Data	**Retention Period OR Criteria Used to Determine Retention Period**
Contact Data	Applicant and employment-related electronic data is retained indefinitely. Paper records are maintained for the duration of employment plus 7 years following employment termination, at which point paper words are destroyed.
Identity Data	Applicant and employment-related electronic data is retained indefinitely. Paper records are maintained for the duration of employment plus 7 years following employment termination, at which point paper words are destroyed.
Government ID Data	Background checks are retained by our vendor for 10 years. Applicant and employment-related electronic data is retained indefinitely. Paper records are maintained for the duration of employment plus 7 years following employment termination, at which point paper words are destroyed.
Biographical Data	Applicant and employment-related electronic data is retained indefinitely. Paper records are maintained for the duration of employment plus 7 years following employment termination, at which point paper words are destroyed.
Transaction and Interaction Data	Applicant and employment-related electronic data is retained indefinitely. Paper records are maintained for the duration of employment plus 7 years following employment termination, at which point paper words are destroyed.
Financial Data	Applicant and employment-related electronic data is retained indefinitely. Paper records are maintained for the duration of employment plus 7 years following employment termination, at which point paper words are destroyed.
Health Data	Applicant and employment-related electronic data is retained indefinitely. Paper records are maintained for the duration of employment plus 7 years following employment termination, at which point paper words are destroyed.
Device/Network Data	Confidential data stored on GeoEngineers information systems

	or portable storage devices is made unreadable to unauthorized parties. Methods include, but are not limited to, strong one-way hash functions, truncation, index tokens, and strong cryptography. GeoEngineers implements automated logging and monitoring controls on its information systems and cloud-based applications that store, process, or transmit electronic data. GeoEngineers internet facing information systems are copied to an alternate secure location, accessible only by authorized parties. Audit and log file information is retained for at least one year.
Inference Data	Applicant and employment-related electronic data is retained indefinitely. Paper records are maintained for the duration of employment plus 7 years following employment termination, at which point paper words are destroyed.
Compliance and Demographic data	Applicant and employment-related electronic data is retained indefinitely. Paper records are maintained for the duration of employment plus 7 years following employment termination, at which point paper words are destroyed.
Protected Category Data	Applicant and employment-related electronic data is retained indefinitely. Paper records are maintained for the duration of employment plus 7 years following employment termination, at which point paper words are destroyed.
Special Category Data	Applicant and employment-related electronic data is retained indefinitely. Paper records are maintained for the duration of employment plus 7 years following employment termination, at which point paper words are destroyed.
Sensitive Personal Information	Applicant and employment-related electronic data is retained indefinitely. Paper records are maintained for the duration of employment plus 7 years following employment termination, at which point paper words are destroyed.

YOUR RIGHTS AND CHOICES

YOUR RIGHTS, INCLUDING YOUR CALIFORNIA PRIVACY RIGHTS

Under the California Consumer Privacy Act ("**CCPA**") and other comprehensive state privacy laws, you may have the following rights, subject to your submission of an appropriately verified request:

Right to Know	You may request any of following, for the 12 month period preceding your request: (1) the categories of Personal Data we have collected about you, or that we have sold, or disclosed for a commercial purpose; (2) the categories

	of sources from which your Personal Data was collected; (3) the business or commercial purpose for which we collected, sold or shared your Personal Data; (4) the categories of third parties to whom we have shared your Personal Data, or disclosed it for a business purpose; and (5) the specific pieces of Personal Data we have collected about you.
Right to Delete	You have the right to delete certain Personal Data that we hold about you, subject to exceptions under applicable law.
Right to Correct	You have the right to correct certain Personal Data that we hold about you, subject to exceptions under applicable law.
Right of Non-retaliation	You have the right to not to receive discriminatory treatment as a result of your exercise of rights conferred by the CCPA.
Minors'	To the extent we have actual knowledge that we collect or maintain Personal Data of a minor under age 16, those minors between the age of 13 and 16 must opt in to any sharing of personal information (as defined under CCPA), and minors under the age of 13 must have a parent consent to sharing of personal information (as defined under CCPA). All minors have the right to opt-out later at any time. Minors under age 13 may have other rights under the Children's Online Privacy Protection Act ("COPPA").

SUBMISSION OF REQUESTS

Current GeoEngineers employees can review much of their Personal Data via the GeoEngineers HR information system.

If you are a current GeoEngineers employee, you can send an email to DataRequest@geoengineers.com to submit requests to exercise your rights in Personal Data subject to this Privacy Notice, to the extent you have those rights under applicable law. You may also contact DataRequest@geoengineers.com for assistance. If you are a contractor, an applicant, former employee, beneficiary, dependent, or family member, please contact us at DataRequest@geoengineers.com for assistance with your privacy requests. For all other questions or comments about this HR Privacy Notice or our privacy practices, please contact DataRequest@geoengineers.com.

VERIFICATION OF REQUESTS

Requests to receive a copy of Personal Data, and requests to delete or correct Personal Data, must be verified to ensure that the individual making the request is authorized to make that request, to reduce fraud, and to ensure the security of your Personal Data. We may require that you provide additional information to verify your identity. If an agent is submitting the

request on your behalf, we reserve the right to validate the agent's authority to act on your behalf.

PROTECTED HEALTH INFORMATION (PHI)

This section describes the legal obligations of GeoEngineers' group health plan (the "Plan") and your legal rights regarding your protected health information held by the Plan under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH Act). Among other things, this Notice describes how your protected health information may be used or disclosed to carry out treatment, payment, or health care operations, or for any other purposes that are permitted or required by law. Since GeoEngineers group health plan is self-insured by the company, we are required to provide this Notice of Privacy Practices (the "Notice") to you pursuant to HIPAA. However, GeoEngineers contracts with a Plan Administrator to manage the day-to-day function of the Plan who. In most cases, the Plan Administrator, not GeoEngineers, has the day-to-day access to your PHI for approving treatment and handling healthcare claims, not GeoEngineers staff directly. Continue reading this notice for details about this access and use of your PHI.

The HIPAA Privacy Rule protects only certain medical information known as "protected health information." Generally, protected health information is health information, including demographic information, collected from you or created or received by a health care provider, a health care clearinghouse, a health plan, or your employer on behalf of a group health plan, from which it is possible to individually identify you and that relates to:

- your past, present or future physical or mental health or condition;
- the provision of health care to you; or
- the past, present or future payment for the provision of health care to you.

If you have any questions about this Notice or about our privacy practices, please contact Jeanna Schmidt, Director of Human Resources, 425.861.6051.

Medical information about employees and covered family members may be used and disclosed by the GeoEngineers group health plan (the "Plan") or others in the administration of your claims.

Our Pledge Regarding Medical Information

We are committed to protecting your personal health information. We are required by law to:

- make sure that any medical information that identifies you is kept private;
- provide you with certain rights with respect to your medical information;
- give you a notice of our legal duties and privacy practices; and

- follow all privacy practices and procedures currently in effect.

How We May Use and Disclose Medical Information About You/Covered Family Members

We may use and disclose your personal health information without your permission to facilitate your medical treatment, for payment for any medical treatments, and for any other health care operation. We will disclose your medical information to Human Resources employees of GeoEngineers for plan administration functions. We will disclose the minimum amount of information necessary for the specific function, and those employees cannot use your information for employment-related purposes. We may also use and disclose your personal health information without your permission for the reasons stated in the Notice and as allowed or required by law. Otherwise, we must obtain your written authorization for any other use and disclosure of your medical information. We cannot retaliate against you if you refuse to sign an authorization or revoke an authorization you had previously given.

Your Rights Regarding Medical Information

You have the right to inspect and copy your medical information to request corrections of your medical information and to obtain an accounting of certain disclosures of your medical information. You also have the right to request that additional restrictions or limitations be placed on the use or disclosure of your medical information, or that communications about your medical information be made in different ways or at different locations.

Excluded Benefits

As referenced in this notice, the "Plan" does not include the following employee welfare benefit plans offered by us:

- Short and long-term disability, group life, voluntary life, long-term care insurance. These plans are governed by the Privacy Practices of the organization providing the benefits referenced here.

Our Responsibilities

We are required by law to:

- maintain the privacy of your protected health information;
- provide you with certain rights with respect to your protected health information;
- provide you with a copy of this Notice of our legal duties and privacy practices with respect to your protected health information; and
- follow the terms of the Notice that is currently in effect.

We reserve the right to change the terms of this Notice and to make new provisions regarding your protected health information that we maintain, as allowed or required by law. If we make any material change to this Notice, we will provide you with a copy of our revised Notice of Privacy Practices by notification through All Staff of updated notice uploaded to company intranet.

Under the law, we may use or disclose your protected health information under certain circumstances without your permission. The following categories describe the different ways that we may use and disclose your protected health information. For each category of uses or disclosures we will explain what we mean and present some examples. Not every use or disclosure in a category will be listed. However, all of the ways we are permitted to use and disclose information will fall within one of the categories.

To Business Associates. GeoEngineers may contract with individuals or entities known as Business Associates to perform various functions on our behalf or to provide certain types of services for the Plan. In order to perform these functions or to provide these services, Business Associates will receive, create, maintain, use and/or disclose your protected health information, but only after they agree in writing with us to implement appropriate safeguards regarding your protected health information. For example, the Plan may disclose your protected health information to a Business Associate to process your claims for Plan benefits or to provide support services, such as utilization management, pharmacy benefit management or subrogation, but only after the Business Associate enters into a Business Associate Agreement with us.

For Treatment. Your protected health information may be used to facilitate medical treatment or services by providers. The Plan may disclose medical information about you to providers, including doctors, nurses, technicians, medical students, or other hospital personnel who are involved in taking care of you. For example, the Plan might disclose information about your prior prescriptions to a pharmacist to determine if prior prescriptions contraindicate a pending prescription. **The use and disclosure of your protected health information will be done through Business Associates who administer the Plan on GeoEngineers' behalf and not by GeoEngineers staff directly**. GeoEngineers staff do not have direct access to your healthcare claims/treatment information, and any information necessary for the administrative function of the Plan is provided via encrypted email to authorized GeoEngineers staff and the Business Associates present this information in a de-identified format, without names or other identifying information.

For Payment. Your protected health information may be used to determine your eligibility for Plan benefits, to facilitate payment for the treatment and services you receive from health care providers, to determine benefit responsibility under the Plan, or to coordinate Plan coverage. For example, the Plan may notify your health care provider about your medical history to determine whether a particular treatment is experimental, investigational, or medically necessary, or to determine whether the Plan will cover the treatment. The Plan may also share your protected health information with a utilization review or pre-certification service provider.

Likewise, the Plan may share your protected health information with another entity to assist with the adjudication or subrogation of health claims or to another health plan to coordinate benefit payments. **The use and disclosure of your protected health information will be done through Business Associates who administer the Plan on GeoEngineers' behalf and not by GeoEngineers staff directly.** GeoEngineers staff do not have direct access to your healthcare claims/treatment information, and any information necessary for the administrative function of the Plan is provided via encrypted email to authorized GeoEngineers staff and the Business Associates present this information in a de-identified format, without names or other identifying information.

For Health Care Operations. Your protected health information may be used for other Plan operations. These uses and disclosures are necessary to run the Plan. For example, your medical information may be used in connection with conducting quality assessment and improvement activities; underwriting, premium rating, and other activities relating to Plan coverage; submitting claims for stop-loss (or excess-loss) coverage; conducting or arranging for medical review, legal services, audit services, and fraud & abuse detection programs; business planning and development such as cost management; and business management and general Plan administrative activities. However, your genetic information will not be used for underwriting purposes. **The use and disclosure of your protected health information will be done through Business Associates who administer the Plan on GeoEngineers' behalf and not by GeoEngineers staff directly.** GeoEngineers staff do not have direct access to your healthcare claims/treatment information, and any information necessary for the administrative function of the Plan is provided via encrypted email to authorized GeoEngineers staff and the Business Associates present this information in a de-identified format, without names or other identifying information.

Treatment Alternatives or Health-Related Benefits and Services. Your protected health information may be used to send you information about treatment alternatives or other health-related benefits and services that might be of interest to you. **The use and disclosure of your protected health information will be done through Business Associates who administer the Plan on GeoEngineers' behalf and not by GeoEngineers staff directly.** GeoEngineers staff do not have direct access to your healthcare claims/treatment information, and any information necessary for the administrative function of the Plan is provided via encrypted email to authorized GeoEngineers staff and the Business Associates present this information in a de-identified format, without names or other identifying information.

As Required by Law. Your protected health information may be disclosed when required by federal, state or local law. For example, when required by national security laws or public health disclosure laws.

For the purpose of administering the plan, certain GeoEngineers Human Resources employees have limited access to your protected health information. However, those employees will only use that information as necessary to perform plan administration functions or as otherwise required by HIPAA, unless you have authorized further disclosures (i.e., if you request

assistance with medical claims or healthcare coverage questions). Your protected health information will never be used for employment action purposes without your specific authorization (e.g., if you request reasonable accommodation or leave of absence for a medical condition).

Special Situations

In addition to the above, the following categories describe other possible ways that we may use and disclose your protected health information without your specific authorization. For each category of uses or disclosures, we will explain what we mean and present some examples. Not every use or disclosure in a category will be listed. However, all of the ways we are permitted to use and disclose information will fall within one of the categories.

Organ and Tissue Donation. If you are an organ donor, the Plan may release your protected health information to organizations that handle organ procurement or organ, eye or tissue transplantation or to an organ donation bank, as necessary to facilitate organ or tissue donation and transplantation.

Military. If you are a member of the armed forces, the Plan may release your protected health information as required by military command authorities. The Plan may also release protected health information about foreign military personnel to the appropriate foreign military authority.

Workers' Compensation. We may release your protected health information for workers' compensation or similar programs, but only as authorized by, and to the extent necessary to comply with laws relating to workers' compensation and similar programs that provide benefits for work-related injuries or illness. For questions about workers' compensation disclosures, contact Lucas Miller, Health and Safety Manager, at 509.209.2830.

Public Health Risks. The Plan may disclose your protected health information for public health actions. These actions generally include the following:

- to prevent or control disease, injury or disability;
- to report births and deaths;
- to report child abuse or neglect;
- to report reactions to medications or problems with products;
- to notify people of recalls of products they may be using;
- to notify a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition;
- to notify the appropriate government authority if we believe that a patient has been the victim of abuse, neglect or domestic violence. We will only make this disclosure if you agree, or when required or authorized by law.

Health Oversight Activities. The Plan may disclose your protected health information to a health oversight agency for activities authorized by law. These oversight activities include, for example, audits, investigations, inspections, and licensure. These activities are necessary for the government to monitor the health care system, government programs, and compliance with civil rights laws.

Lawsuits and Disputes. If you are involved in a lawsuit or a dispute, the Plan may disclose your protected health information in response to a court or administrative order. The Plan may also disclose your protected health information in response to a subpoena, discovery request, or other lawful process by someone else involved in the dispute, but only if efforts have been made to tell you about the request or to obtain an order protecting the information requested.

Law Enforcement. The Plan may disclose your protected health information if asked to do so by a law enforcement official—

- in response to a court order, subpoena, warrant, summons or similar process;
- to identify or locate a suspect, fugitive, material witness, or missing person;
- about the victim of a crime if, under certain limited circumstances, we are unable to obtain the victim's agreement;
- about a death that we believe may be the result of criminal conduct; and
- about criminal conduct

Coroners, Medical Examiners and Funeral Directors. The Plan may release protected health information to a coroner or medical examiner. This may be necessary, for example, to identify a deceased person or determine the cause of death.

National Security and Intelligence Activities. The Plan may release your protected health information to authorized federal officials for intelligence, counterintelligence, and other national security activities authorized by law.

Inmates. If you are an inmate of a correctional institution or are under the custody of a law enforcement official, the Plan may disclose your protected health information to the correctional institution or law enforcement official if necessary (1) for the institution to provide you with health care; (2) to protect your health and safety or the health and safety of others; or (3) for the safety and security of the correctional institution.

Required Disclosures

The following is a description of disclosures of your protected health information we are required to make.

Government Audits. The Plan is required to disclose your protected health information to the Secretary of the United States Department of Health and Human Services when the Secretary is investigating or determining our compliance with the HIPAA privacy rule.

Disclosures to You. When you request, the Plan is required to disclose to you the portion of your protected health information that contains medical records, billing records, and any other records used to make decisions regarding your health care benefits. The Plan is also required, when requested, to provide you with an accounting of most disclosures of your protected health information if the disclosure was for reasons other than for payment, treatment or health care operations, and if the protected health information not disclosed pursuant to your individual authorization.

Other Disclosures

Personal Representatives. The Plan will disclose your protected health information to individuals authorized by you, or to an individual designated as your personal representative, attorney-in-fact, etc., so long as you provide us with a written notice/authorization and any supporting documents (i.e., power of attorney). Note: Under the HIPAA privacy rule, we do not have to disclose information to a personal representative if we have a reasonable belief that:

- you have been, or may be, subjected to domestic violence, abuse or neglect by such person;
- treating such person as your personal representative could endanger you; or
- in the exercise or professional judgment, it is not in your best interest to treat the person as your personal representative.

Spouses and Other Family Members. With only limited exceptions, the Plan will send all mail to the employee. This includes mail relating to the employee's spouse and other family members who are covered under the Plan and includes mail with information on the use of Plan benefits by the employee's spouse and other family members and information on the denial of any Plan benefits to the employee's spouse and other family members. If a person covered under the Plan has requested Restrictions or Confidential Communications (see below under "Your Rights"), and if we have agreed to the request, the Plan will send mail as provided by the request for Restrictions or Confidential Communications.

Authorizations. Other uses or disclosures of your protected health information not described above will only be made with your written authorization. For example, in general and subject to specific conditions, the Plan will not use or disclose your psychiatric notes; the Plan will not use or disclose your protected health information for marketing; and the Plan will not sell your protected health information, unless you give us a written authorization. You may revoke written authorization at any time, so long as the revocation is in writing. Once we receive your written revocation, it will only be effective for future uses and disclosures. It will not be effective for any information that may have been used or disclosed in reliance upon the written authorization and prior to receiving your written revocation.

Your Rights

You have the following rights with respect to your protected health information:

Right to Inspect and Copy. You have the right to inspect and copy certain protected health information that may be used to make decisions about your Plan benefits. If the information you request is maintained electronically, and you request an electronic copy, the Plan will provide a copy in the electronic form and format you request, if the information can be readily produced in that form and format; if the information cannot be readily produced in that form and format, we will work with you to come to an agreement on form and format. If we cannot agree on an electronic form and format, we will provide you with a paper copy.

To inspect and copy your protected health information, you must submit your request in writing to Jeanna Schmidt, Director of Human Resources, 425.861.6051. Your request will be submitted to the Business Associate who administers the Plan for GeoEngineers; Business Associates may require additional information directly from you to complete your request. If you request a copy of the information, we or the Business Associate may charge a reasonable fee for the costs of copying, mailing or other supplies associated with your request.

Right to Amend. If you feel that the protected health information the Plan has about you is incorrect or incomplete, you may request an amendment to the information. You have the right to request an amendment for as long as the information is kept by or for the Plan.

To request an amendment, you must make your request in writing to Jeanna Schmidt, Director of Human Resources, 425.861.6051. In addition, you must provide a reason that supports your request. Your request will be submitted to the Business Associate who administers the Plan for GeoEngineers; Business Associates may require additional information directly from you to complete your request.

Your request may be denied if you ask us to amend information that:

- is not part of the medical information kept by or for the Plan;
- was not created by the Plan, unless the person or entity that created the information is no longer available to make the amendment;
- is not part of the information that you would be permitted to inspect and copy; or
- is already accurate and complete.

If your request is denied, you have the right to file a statement of disagreement with us and any future disclosures of the disputed information will include your statement.

Right to an Accounting of Disclosures. You have the right to request an "accounting" of certain disclosures of your protected health information. The accounting will not include:

- disclosures for purposes of treatment, payment, or health care operations;
- disclosures made to you;

- disclosures made pursuant to your authorization;
- disclosures made to friends or family in your presence or because of an emergency;
- disclosures for national security purposes; and
- disclosures incidental to otherwise permissible disclosures.

To request this list or accounting of disclosures from the Plan, you must submit your request in writing to Jeanna Schmidt, Director of Human Resources, 425.861.6051. Your request must state the time period you want the accounting to cover, which may not be longer than six years before the date of the request. Your request should indicate in what form you want the list (for example, paper or electronic). Your request will be submitted to the Business Associates from whom GeoEngineers would obtain the accounting of disclosures. The first list you request within a 12-month period will be provided free of charge. For additional lists, we may charge you for the costs of providing the list. We will notify you of the cost 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 your protected health information that the Plan uses or discloses for treatment, payment or health care operations. You also have the right to request a limit on your protected health information that the Plan discloses to someone who is involved in your care or the payment for your care, like a family member or friend. For example, you could ask that the Plan not use or disclose information about a surgery that you had.

Except as provided in the next paragraph, the Plan is not required to agree to your request. However, if we do agree to the request, we will honor the restriction until you revoke it or we notify you.

We will comply with any restriction request if (1) except as otherwise required by law, the disclosure is to the health plan for purposes of carrying out payment or health care operation (and is not for purposes of carrying out treatment); and (2) the protected health plan information pertains solely to a health care item or service for which the health care provider involved has been paid in full by you or another person.

To request restrictions, you must contact the Business Associate who administers the Plan for GeoEngineers.

Right to Request Confidential Communications. You have the right to request that the 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 request confidential communications, you must contact the Business Associate who administers the Plan for GeoEngineers.

Right to Be Notified of a Breach. You have the right to be notified in the event that we (or a Business Associate) discover a breach of unsecured protected health information.

Right to a Paper Copy of This Notice. You have the right to a paper copy of this notice. You may ask us 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.

You may obtain a copy of this notice on GeoEngineers' intranet.

To obtain a paper copy of this notice, contact Jeanna Schmidt, Director of Human Resources, 425.861.6051.

Complaints

If you believe that your privacy rights have been violated, you may file a complaint with the Plan or with the Office for Civil Rights of the United States Department of Health and Human Services. To file a complaint with the Plan, contact Jeanna Schmidt, Director of Human Resources, 425.861.6051. All complaints must be submitted in writing. A complaint to the Office of Civil Rights should be sent to:

Region X – Seattle (Alaska, Idaho, Oregon, Washington)
Office for Civil Rights
U.S. Department of Health and Human Services
2201 Sixth Avenue - M/S: RX-11
Seattle, WA 98121-1831
Voice Phone (206)615-2290
FAX (206)615-2297
TDD (206)615-2296

You will not be penalized, or in any other way retaliated against, for filing a complaint with the Office of Civil Rights or with us.