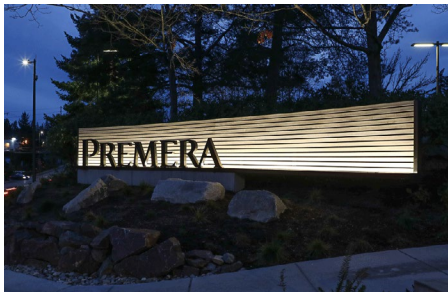
CODE OF CONDUCT



PREMERA | BLUE CROSS BLUE SHIELD OF ALASKA

Why it matters

— A LETTER FROM OUR CORPORATE COMPLIANCE AND ETHICS OFFICER —

Compliance and ethics — why they matter

Sven Peterson
Corporate Compliance and Ethics Officer, and VP of Compliance, Ethics and Regulatory Services

Dear Employee,

At Premera we are unwavering in our commitment to comply with the highest standards of ethical behavior. We do so because every decision we make has a direct impact on our customers, the providers we partner with, the employees we work with, and the communities we serve. People rely upon us during many of the most important times in their lives. Our expectation is that all employees conduct themselves with the highest standards of integrity and ethics.

Being a part of an ethical organization with an inclusive workplace that embraces mutual understanding and respect makes me proud. The Premera Code of Conduct reflects these commitments. We hold ourselves to the standards set forth within it. I encourage you to spend time reading and understanding it. Discuss its meaning with your colleagues.

Doing the right thing and maintaining a culture of ethics and compliance is often difficult. It requires us to work together to hold ourselves accountable. If you see something that concerns you, I encourage you to speak up. Talk to your leader or reach out to our Compliance and Ethics team. You can also reach out to me directly.

Although our Code of Conduct applies to our employees, we publish it on our website and make it available publicly. We want our customers, provider partners, regulators, lawmakers, and fellow members of our community to know the commitments that we are making. By being an ethical company, we make healthcare work better and earn their trust.

Thank you for your commitment to maintaining our culture of ethics and compliance, and for your service to our customers and community.

Sincerely,
Sven Peterson
Corporate Compliance and Ethics Officer
Vice President of Ethics, Compliance and Regulatory Services

*Premera refers to PREMERA and its affiliated companies, excluding Practice Management Group, LLC (PMG).

Contents

Contents

Purpose and values

Purpose and values

Our purpose

Improve customers' lives by making healthcare work better. How do we do this? By applying our values to the work we do—every single day. These values offer a roadmap for how we conduct business, treat each other, and treat our customers. Our Code of Conduct outlines how we use our values to make decisions and work with each other internally. It also governs how we treat those we serve. This includes customers, providers, third parties, regulators, and the employers that use our services. Our commitment to Do the Right Thing runs deep. It serves as a cornerstone of our Compliance and Ethics Program. We pledge to always conduct ourselves legally, ethically, and with unwavering integrity. We endeavor to build trust in every relationship we forge and each life we touch.

OUR CUSTOMERS WILL SAY:

You take great care of me and make it simple and easy.

Our values

Do the Right Thing

Identify with the Customer

Act with Urgency

Be Excellent

Challenge Convention

Work Together

To ensure our continued success, we must focus on **how** we achieve our business objectives. This means looking beyond our short-term goals. So, Premera has established core values to guide how we work. This builds trust in our relationships with customers, providers, third parties, and regulators. We expect all Premera employees to exhibit these shared values as we perform our work every day. This extends to all people authorized to act on the company's behalf.

Do the Right Thing. Simple words that are the foundation for Premera's Compliance & Ethics Program. This Code of Conduct (the Code) models our commitment to doing the right thing. It also shows our focus on always conducting business legally and ethically. As we work together to make healthcare work better, we turn to the Code as our formal declaration. **We commit to always and enthusiastically Do the Right Thing.** This is our duty to our Board of Directors, external committee members, customers, constituents, and employees.

Our responsibilities

Our responsibilities

We're committed to upholding the principles outlined in our Code of Conduct. We also uphold our corporate and departmental policies and the laws that govern us. By following these principles, we safeguard our own integrity. We also nurture a culture of trust and accountability within Premera.

We recognize that speaking up is an act of courage and responsibility. So, we encourage every employee to report any suspected violations. They may report to their manager, Regulatory Compliance & Ethics, or the Employee Experience departments. Employees can also use the C&E hotline. Voicing concerns can be challenging. That's why we provide the Compliance & Ethics Hotline. It's a confidential reporting system managed by a trusted third party. Premera does not tolerate retaliation or intimidation. We protect those who act in good faith or take part in an investigation.

We expect employees to do the following:

- Let ethics guide all business decisions. We never compromise our integrity or ask others to commit unethical or illegal acts.
- Be informed of laws, regulations, and policies. We all have a duty to comply with applicable laws.
- When in doubt, ask! Employees should promptly discuss ethical or compliance concerns or questions. They can do this with their manager, Regulatory Compliance & Ethics, or their HR business partner. We encourage questions and concerns. **Together we can navigate ethical decision-making to always Do the Right Thing.**

Q: I am new in my role, and it is unclear whether a process I am responsible for is compliant with various requirements. What can I do about it?

A: Talk to your manager. If you are not comfortable doing that, talk to the next level of management, contact Regulatory Compliance & Ethics or Employee Experience. Another option available to you is to use the Compliance & Ethics Hotline. Open discussions of ethics strengthen our culture at Premera.

Our responsibilities

Leader responsibilities

Our leaders play an important role in fostering our culture of ethics and compliance. Leaders ensure their teams uphold the principals outlined in the Code of Conduct. They serve as role models of appropriate behavior and set a good example.

We expect leaders to follow these guidelines:

- Embrace our Code and make sure employees understand the behaviors expected of them.
- Create a positive environment. Employees should feel comfortable raising concerns or challenging questionable conduct. When an employee raises a concern, ensure that it is investigated. If you're unsure about what to do, reach out to Regulatory Compliance & Ethics or Employee Experience for help.
- Be transparent. Never disregard ethical standards to achieve any business objective or personal goal.
- Recognize and reward employees whose behavior demonstrates our values. This creates a ripple effect that inspires others to follow suit.
- Report known or suspected non-compliance, fraud, waste, and abuse (FWA), or Code violations immediately.
- Model behaviors. This means that we show personal accountability and ensure our own actions align with Premera's values and ethical standards.
- Follow our non-retaliation policy. Periodically remind employees about this policy. Reinforce our values and encourage employees to speak up when they suspect something is wrong.
- Ensure their teams complete all mandatory trainings, required disclosures, and certifications in a timely manner.
- Monitor the business partners, contractors, and contingent workers they engage with. Ensure their conduct is consistent with our Code.

Our pledge to respond

If you know or suspect an incident of non-compliance, fraud, waste, and abuse (FWA), or a Code violation, report it immediately. Don't ignore the issue, wait to confirm, or consult a coworker.

The Regulatory Compliance & Ethics department reviews and investigates reported potential Code violations. We partner with Employee Experience. They review and consider all relevant information. They may involve other departments if necessary.

The Corporate Compliance & Ethics Officer directs the investigation. They report the results to the Audit and Compliance Committee of the Board of Directors, or the full Board of Directors. They also report Code violations to appropriate regulatory agencies or business partners. This includes violations of law, regulation, and applicable government contracts.

Compliance with the law

"Our deeply rooted commitment to Doing the Right Thing and Being Operationally Excellent is essential to maintaining a strong reputation with our customers and our regulators."

— Kitti Cramer, EVP, Chief Legal & Risk Officer

Compliance with the law

All Premera employees must know and understand the laws that affect their business area. Failure to follow a law could result in fines and penalties for Premera. It can also damage the trust we've worked so hard to build over time. Employees who do not follow applicable laws and regulations could be subject to corrective action. This could include job loss and criminal charges or prosecution.

Reporting fraud committed against Premera

Each employee plays a crucial role in preventing, detecting, and reporting non-compliance, and possible fraud, waste, and abuse (FWA). If you suspect fraudulent activity, report it to the Special Investigations Unit (SIU) or Internal Audit Department. They will investigate the matter. If funds are missing, Premera will attempt to recover them and contact the proper authorities.

See **Appendix A** for links to laws that apply to fraud, waste and abuse. We all have a duty to follow these laws. Review **Appendix B** for the Definitions and Key Indicators of potential FWA for customers, providers, pharmacies, wholesalers, manufacturers, plan sponsors, producers, and employees.

Together we form a collective that safeguards Premera's resources and reputation. We also reinforce our commitment to ethical conduct.

To report suspected FWA events and activities related to external parties (such as a provider, pharmacy, or member), complete the Referral for Potential Fraud form and email it to Stop Fraud or call the Anti-Fraud Hotline.

To report potential fraud by a Premera employee, contact the Internal Audit Department or call the Compliance & Ethics Hotline to report anonymously.

Management-level employees who are informed, or otherwise become aware, of suspected internal fraud must immediately report the suspected internal fraud to Internal Audit.

Q: How can I learn what laws and regulations apply to my area?

A: Be familiar with the corporate and departmental policies that are applicable to your job function. All corporate policies can be found on the Corporate Policies internal website. Individual departments are responsible for creating, maintaining, distributing, and sharing departmental policies and changes to employees.

Compliance with the law

Nondiscrimination of services or healthcare benefits

We are committed to a culture of integrity, ethical conduct, and compliance with all state and federal laws and applicable regulations. We stand firmly against any form of discrimination. We will not discriminate based on race, color, ethnicity, national origin, sex, gender identity or expression, marital status, age, sexual orientation, disability, language fluency, religion, genetic information, veteran status, or other protected categories under federal, state, or local law.

Through awareness and understanding, we create a work culture where everyone is valued, respected, and treated fairly. Each of us can contribute our unique perspective and talent. Together we foster an atmosphere of trust, collaboration, and mutual respect. This ensures that Premera is an inclusive and welcoming place for all.

Doing business with the government

Premera recognizes the importance of its partnerships with federal, state, and local governments. Doing business with the government means we have to strictly follow special laws and regulations. The consequences for violating these legal requirements can be severe.

Please note that employees of the Federal Employee Program's Director's Office of the Blue Cross Blue Shield Association are not considered government employees. However, it remains crucial to avoid any perception of conflicts of interest to uphold the highest standards of integrity.

It's vital to understand how we work with the government. Refer to **Appendix A** for a list of the major federal laws that apply to Premera based on the federal programs in which we participate. These guidelines help us navigate our specific requirements and obligations.

Offering gifts or business courtesies to government employees

Premera employees are forbidden from offering any money, gifts, services, or entertainment to government employees. Contact Regulatory Compliance & Ethics with any question about these requirements.

Anti-slavery and human trafficking

We ensure our operations and supply chains are free from the practices of slavery and human trafficking, and we comply with all relevant labor standards.

Q: I work in Claims and have been working very closely with someone from Centers for Medicare & Medicaid Services (CMS). She has been very helpful in explaining how we need to handle secondary payments. Can I send her a small gift to thank her?

A: No, you can't send anything of monetary value to a government employee. Sending a nice thank you card or email would be appropriate.

Compliance with the law

Being excluded from government programs

Some Premera employees may not be able to work with government programs, such as Medicare Advantage. Any employee who has been debarred, excluded, or suspended from working with any governmental agency must immediately notify Regulatory Compliance & Ethics.

This is important since Medicare and other federal healthcare programs will delay payment for services performed or ordered by anyone who has been excluded from working with any government agency. We regularly review published information for excluded individuals and entities. Anyone on the list that is employed or retained by Premera is notified and given the opportunity to provide proof that they are not excluded. Exceptions may be made for sanctioned providers if they do not participate in a federal or federally funded healthcare program.

Employing government personnel

Former government employees may be restricted in the type of employment they can accept. These rules depend on the agency involved, the type of position that was held, and the potential position at Premera.

Before interviewing or making a job offer to a former or current government employee, work with Employee Experience to determine if their previous government employment could be a conflict of interest. See Hiring Current or Former Government Employees policy.

Preparing and submitting accurate reports

Federal and state healthcare programs have strict reporting requirements. All proposals, budgets, financial data, and reports created as part of these programs must be accurate, complete, and subject to appropriate management review. Supporting records must be retained in accordance with our record retention requirements. Anyone submitting false data to the government could face severe sanctions.

These requirements also apply to time reporting and expense reports. Specific rules cover what costs may be charged and how they can be allocated. Any costs charged to the government must be accurate and appropriately supported.

By following these reporting guidelines, we commit to maintaining integrity and accountability.

Q: I work in Finance and am responsible for preparing a regulatory filing every month. We recently changed systems and I'm concerned the data is incomplete. What should I do?

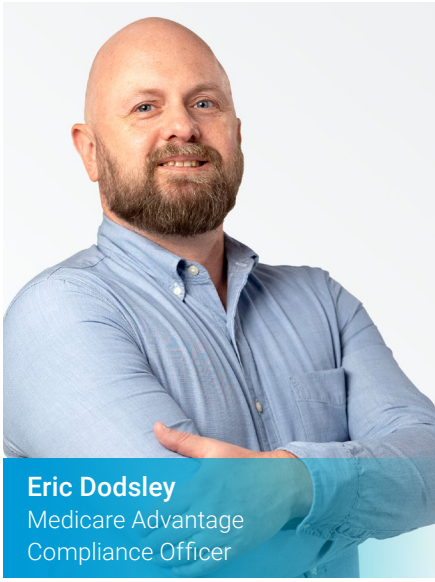
A: Discuss the situation with your manager. If there are differences between what you used to report and what you are currently reporting, there could be data that wasn't accurately converted. This needs to be resolved immediately, and any past reports with inaccurate data should be resubmitted. Contact Regulatory Compliance & Ethics for additional guidance.

Compliance with the law

Government requests for information

We take a cooperative approach when we receive reasonable requests from federal, state, and local authorities for information. For example, Premera may be asked for protected personal information (PPI) that is protected by federal and state privacy laws. In this case, we would be required to ensure that the agency is allowed to receive PPI. If possible, we may request special protection for the PPI.

Anyone who receives a request for information, either on our campuses or outside the workplace, must contact Regulatory Compliance & Ethics to help respond appropriately. Anyone who receives a request for employment information for a current or former Premera employee must contact Employee Experience. Communication with these departments helps us handle these requests correctly.



Eric Dodsley
Medicare Advantage Compliance Officer

Medicare Advantage requirements and responsibilities

Employees and Board Members must complete Medicare Advantage compliance, fraud, waste, and abuse (FWA), and job-specific compliance training and education. We all have a duty to comply with the legal requirements of the Medicare Advantage program.

Fair competition

We are committed to following federal antitrust and state fair competition laws. We are forbidden from doing the following:

- Discussing pricing, bids, discounts, promotions, and costs with competitors.
- Making agreements with competitors to allocate customers or divide markets (territories).
- Discriminating for or against customers on any basis other than underwriting criteria.
- Making false or deceptive statements about our products or services.

Before considering any type of arrangement with competitors, consult with Legal or Enterprise Vendor Management and Contracting.

Compliance with the law

Political activity, lobbying, and contributions

As residents of this country, we enjoy the privilege of engaging in the political process. We encourage everyone to be active in this process, but all political activity must be conducted outside of working hours and away from our campuses.

All political activity and political contributions on behalf of Premera must be coordinated through Congressional and Legislative Affairs. Unless it is a Premera-sponsored activity, employees must not act in the following ways:

- Represent or appear to represent Premera if they are not approved to do so.
- Seek payment or reimbursement of campaign contributions or fundraising costs.
- Use Premera property or employees for campaign activity. Examples include using our equipment to send invitations for fundraising events or assisting in a campaign during work hours.

All lobbying on behalf of Premera must be coordinated through Congressional and Legislative Affairs. Unless approved by the vice president of congressional and legislative affairs, employees must not do these things:

- Contact government officials about Premera's position on legislation, regulations, or other policies.
- Represent or negotiate Premera's position on developing legislative language to industry colleagues, trade associations, or other interested parties.

Q: Someone who said they are from the Office of the Insurance Commissioner (OIC) called me at work today and asked a bunch of questions about one of our new products. I didn't know who it was so I told them I'd have to call them back. Was that okay?

A: Yes, that was the appropriate action to take. Whenever you receive a request from someone stating that they are from a state or federal insurance department, you must refer the call to Regulatory Compliance & Ethics unless you have been authorized to answer inquiries previously. Please contact Legal or Regulatory Compliance & Ethics for additional assistance.

Media relations

Our reputation is one of our most valuable assets. To protect it, Corporate Communications oversees all contact with the media. If someone from a media organization contacts you seeking Premera's position on an issue, policies, or practices, do not make any comments. Refer them to Corporate Communications. All news releases concerning Premera must be approved by Corporate Communications. For more information about interacting with the media, contact Corporate Communications.

Trademark and brand usage

Third parties have an interest in leveraging their relationship with Premera and will occasionally ask for endorsements or permissions to use our trade names and logos. We have strict guidelines on these actions and any requests from third parties must be reviewed and approved by our Brand Creative and Legal departments in advance of any such use.

Protecting our data

"Privacy is about trust. If we don't protect our customers' most valuable information, we won't have their trust or their business."

— Chris Brandt, Privacy Official

Protecting our data

Accuracy of records

Premera expects all records to be properly recorded and authorized by management. For example, making records appear as though payments were made to one person when, in fact, they were made to another, or submitting expense reports that do not accurately reflect the true nature of an expense, is not allowed.

Providing false information, verbally or in writing, is also prohibited. This includes intentionally misrepresenting facts during investigations, audits, process reviews, and any other fact-finding efforts taken on behalf of Premera or any regulators examining Premera. As with everything else we do, record keeping must be driven by honesty, authenticity, and integrity.

Electronic communications

Premera provides email, chat, and video conferencing software for business purposes. All use must follow corporate and departmental policies. We reserve the right to monitor and disclose the contents of electronic media and communications, where permitted by law.

We must not use Premera resources to send offensive communications. This includes jokes or graphics that would violate our policies regarding unlawful retaliation, harassment, and discrimination. We should treat others as they want to be treated. Conduct all communications in a professional and respectful manner.

Using company assets

Part of delivering excellent service means using Premera's assets in the way they are intended to be used. These assets include, but are not limited to the following:

- Equipment
- Company property and buildings
- Corporate funds
- Office supplies
- Employees' work time
- Business strategies and plans
- Financial data, records, and work files
- Other confidential information about our business and our customers

We must not use our assets for personal gain or for the benefit of others. Because such assets belong to Premera, they should not be transferred to others outside the course of normal business. For more information, see our Company Access to Information and Property Policy.

Q: What should I do if I suspect my manager is using company funds for personal use?

A: Employees with a reasonable belief that internal fraud has occurred have a responsibility to report such incidents to the Internal Audit Department. Premera prohibits employees from engaging in retaliation, retribution, or any form of harassment against an employee for reporting fraud-related issues or concerns in good faith, or for cooperating with an investigation.

Protecting our data

Premera, like other healthcare organizations, is frequently targeted by attackers who want to steal data or disrupt our operations. To protect our members' sensitive information and ensure that we can provide uninterrupted service, it's important that all employees follow our cybersecurity policies, which include the following:

- Access Permissions
- Computer, Network, and Telephone Usage
- Computer Passwords
- Cybersecurity Incident Response
- Device and Media Controls
- Email and Other Electronic Communications
- Cryptography

Protecting our data

Premera's confidential information

Much of what we handle as employees is confidential and subject to government regulations. Private information includes Premera customer information and any information about our business, our employees, or any third party doing business with Premera that is not generally available to the public.

Confidentiality is key to how we conduct business. Improper use or disclosure of this information could cause harm to the company. We all need to actively protect Premera's confidential information. **Do the Right Thing** continues even after an employee leaves Premera.

Examples of Premera's confidential information include, but are not limited to:

- Protected personal information (PPI), which includes protected health information (PHI)
- Financial data
- Internal systems data
- Pricing or product information
- Sales and marketing figures
- Underwriting information
- Lists of customer groups or individuals
- Changes in management or policies
- Provider reimbursement or contracting information
- Information about Premera's relationships with government and regulatory agencies, as well as public and private organizations
- Plans for improving any of our products or services
- Confidential customer information
- Vendor contracts, terms, and pricing

Q: Is it okay to share Premera information with my sister who works at Kaiser Permanente and could use the help to do her job?

A: No, you must not use or share such information for any purpose other than to perform your job functions. You should take necessary precautions to prevent the unplanned disclosure of confidential information to others.

Please note, if a family member works for a competitor or supplier, including any provider of medical services, or is employed by a governmental agency that may interact with Premera, it must be fully disclosed to Regulatory Compliance & Ethics.

Premera's trade secrets

Some employees will have access to trade secrets. It's important that these not be shared. The Washington Uniform Trade Secrets Act (WUTSA), located at Chapter 108 of Title 19 of the Revised Code of Washington, protects our company's trade secrets. This includes an employee's work on confidential projects and business strategies for Premera. The WUTSA prohibits employees from disclosing not only written or electronic documents, but also information recreated from memory. Employees' must continue to protect Premera's trade secrets even after they stop working with Premera.

Protecting our data

Protecting PPI and confidential information

Employees need to safeguard the confidential and protected personal information (PPI) of our members. This requires constant care and vigilance. It's something that we take seriously. For example, we should always be careful to avoid discussing matters related to work being done at Premera in public places and even in the common areas within our buildings. We must make sure that discussions involving member PPI or confidential information only occur around employees authorized to have access to such information and who need to know the information to carry out their duties for Premera.

Chris Brandt
Privacy Official

Marking documents

One way to protect confidential information is to ensure it is properly marked. The chart below contains basic information about marking documents. For additional information, please see our Marking Guidelines.

Document is created under attorney-client privilege	Document contains customer PPI	Document contains employee PPI	Document is highly confidential	Document is intended for internal use only
YES	YES	YES	YES	YES
Attorney-client privileged or attorney work product	Confidential PPI—customer	Confidential PPI—employee-restricted	Confidential and proprietary—restricted solely for authorized persons having a need to know	Confidential and proprietary—for internal use only OR confidential and proprietary

If content is intended for public viewing, ensure it contains appropriate Premera branding.

Retention of records

Laws and regulations govern the length of time we must retain company records. If Premera is involved in a lawsuit or a government investigation or audit, related records must not be destroyed until the matter is closed. Destroying or changing documents related to a legal or regulatory matter is forbidden.

Before destroying any records, refer to the Records Management policy. Employees can also consult with their records coordinator or visit the Data Governance site.

Protecting our data

Employees' confidential information

Just as we take the confidentiality of customer information seriously, we do the same for our employees. We take necessary steps to prevent the accidental disclosure of employee information to others. Private employee information includes, but is not limited to these examples:

- Medical or claims information
- Social Security and bank account information
- Wage and salary information
- Performance information
- Reasons for termination of employment
- Demographic information such as age and address
- Other personal information

Only people who are authorized to process employee claims should have access to a limited subset of employee data to perform their duties. Employees may not have access to their data or their family members' data. Employees may not review the data of a family member or even their own data as part of their work. If such information is needed, it must be accessed only through the member portal on the Premera member website. Anyone who has access to employee data without being on the authorized list of users should email the Group 14-16 mailbox immediately. Employees with past access who no longer need access to this data should have their manager submit a ServiceNow ticket to remove access.

Confidential information of third parties

Protecting confidential information about our third-party partners is just as important as what we do for our members and employees. These partners include suppliers and vendors. We project this type of information, including trade secrets, for our third-party vendors.

For example, laws prohibit employees' unauthorized disclosure or use of another company's trade secrets. Employees should also honor any contractual commitments they may be subject to that prohibit disclosure or use of any former employer's confidential or proprietary information.

Protecting our data

Insider trading

Although Premera is not a publicly traded company, employees may become aware of non-public or "inside" information about other companies that may affect an investor's decision to buy or sell investments. Employees who become aware of such information may not use it to buy or sell securities of that company and may not share that information with others.

Customer privacy

We follow federal and state privacy laws, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This law protects the financial and health information of our members. We use the following privacy principles to guide our actions:

Customers: Customers should enjoy the full array of privacy protections afforded to them by law and routinely granted by their providers. This is a values-based approach focused on our primary core value: Do the Right Thing.

Employers: Employers that contract with Premera are not allowed to view all the health data of their employees. We will provide the level of employee health information to employers and producers (also known as brokers or agents) based on the specific employer contract. Refer questions to the Privacy Program staff.

We create, collect, receive, maintain, transmit, use, and disclose protected personal information (PPI), such as name, date of birth, address, and claim information, to pay claims and otherwise serve our customers. We work diligently to comply with federal and state privacy laws that govern the ways we handle our customers' PPI. Before handling this type of information, employees should discuss it with their department's privacy liaison or Premera's Privacy Program staff.

Where appropriate, we use technical and/or physical security safeguards, such as encrypted emails, badges to enter our buildings, and security guards, to ensure our privacy policies are followed.

Q: Whom can I contact with Privacy questions?

A: Your manager, your department Privacy Liaison.

Q: Whom can I contact with security questions?

A: You can email Information Security Awareness to reach the Cybersecurity department.

Q: Someone walked in the door behind me without "badging" in. Is that okay?

A: No, you should question the presence of the individual. Report the incident to Security immediately.

Protecting our data

Employee privacy

Premera maintains a culture of the highest ethical standards to protect the privacy and security of our technology resources. We expect company resources to be used in ways that are consistent with our business interests and align with this Code of Conduct.

Employees may have access to Premera technology resources to conduct business on behalf of Premera and are responsible for following all policies, procedures, and standards. All Premera technology resources and the data stored on them are always the property of Premera. Anyone with access to Premera technology resources should not expect privacy when using company equipment. It's also important to know that any activity using Premera technology resources may be monitored at any time without notice.

Customer security

We are committed to ensuring the security of our facilities and electronic systems to prevent unauthorized access to Premera's and our customers' protected personal information (PPI).

We are expected to be aware of and follow established corporate and departmental policies, processes, and procedures that are designed to secure our buildings and electronic systems in compliance with HIPAA security requirements. We are all responsible for maintaining the security of our campuses and buildings.

Social media, cloud storage, file transfer, and artificial intelligence tools

Employees are not allowed to use company assets to access and use social media sites, cloud storage sites, file transfer websites, or AI or machine learning technologies (such as generative AI) that are not approved by Premera. Widespread use of such sites in the workplace can lead to increased risk of unauthorized disclosure of PPI, as well as increased risk of a malicious software infection.

Corporate Communications decides who, officially, represents Premera and may post information to social media sites about our company and our products. This includes answering questions from customers and other consumers. Employees who do not officially represent Premera should ensure that any comments made about Premera are clearly labeled as personal comments. Employees who have been approved to access social media sites from Premera assets are expected to use their best judgment, just as when using the phone or email. When in doubt, employees should discuss performance expectations with their manager.

Q: If I need to send a file for business purposes that is too big to send via email, what should I do?

A: Never upload PPI or other business information to a file transfer website unless this has been specifically approved. Check with your manager or your department's privacy liaison if you aren't sure. Instead, open a ServiceNow ticket with the Electronic Transmission Center for assistance with other secure options.

Q: Who can I talk to for more information about social media?

A: You can contact Corporate Communications.

Protecting our data

Using and choosing images

Use good judgment when posting images such as clip art and photographs or including them in emails or other communications. Employees who take photographs in the workplace and share them online should ensure that no work products, including images such as computer screens, team noticeboards, and company documents, are visible. Additionally, no pictures of other employees should be shared without their permission.

Many of our corporate and departmental policies apply to online activities, such as the prohibition on sharing PPI. Specifically, employees must not disclose PPI or any other Premera confidential or proprietary information online. Just as PPI may never be sent via email without first being marked "confidential" to encrypt and secure it, PPI may never be sent to either an internal or external recipient via an internet file-transfer cloud service website that is not specifically approved for that purpose by Cybersecurity. Uses or disclosures of PPI that are allowed by corporate and departmental policy, but that are too large to be transferred by confidential email or other secure electronic channels, should be done through the Electronic Transmission Center.

Adrian Mayers
VP and Chief Information Security Officer

"Our unwavering commitment to understanding and supporting our customers' needs makes it clear that protecting their personal information is vitally important."

– Dr. Adrian M. Mayers, Chief Information Security Officer

Conflicts of interest

"When we work together, the whole is greater than the sum of the parts."

— Dave Braza, EVP, Healthcare Informatics & Chief Actuary

Conflicts of interest

Duty of professional loyalty and conflicts of interest

We value loyalty and are responsible for preventing outside activities, personal interests, and relationships from impacting the decisions we make when performing our duties as employees. All employees and others engaged to perform services on our behalf are expected to be loyal and to avoid conflicts of interest. This means business decisions must be based on the best interests of Premera and should not be motivated by personal desires or relationships.

Conflicts of interest can happen if an employee's activities or interests influence or appear to influence their job performance. Many situations can cause a conflict of interest. Conflicts can be difficult to detect and are often judgment calls between what is acceptable and unacceptable. The existence of a potential conflict may not mean the outside activity or relationship must end. In many cases, steps can be taken to prevent the conflict from impacting your work.

Each employee must avoid actual conflicts as well as the appearance of a conflict. Review this Code and related policies to identify possible conflicts. We rely on each employee to disclose any relationships that could be misinterpreted as a conflict. This includes, but is not limited to, relationships with the following entities:

- Customers
- Providers
- Third parties
- Non-employees, which includes contingent workers and outsourced service workers
- Business partners (such as producers, also known as brokers or agents)
- Competitors
- Other employees

Employees with questions about an activity, situation, or relationship that might cause a conflict of interest should discuss it with their manager. If a potential conflict exists, it must be reported to Regulatory Compliance & Ethics. Early reporting allows for timely resolution. Therefore, don't wait until the annual Conflict of Interest process to report. We will work together to develop a plan to address the conflict.

Duty to report and disclose relationships

Conflicts of interest can also exist in relationships between employees. Employees are not allowed to supervise or work for a family member or someone with whom they have a close personal relationship. This could create the perception of favoritism or special treatment. Should a close personal relationship develop after the reporting relationship is formed, discuss this with management and Employee Experience.

Employees whose family member(s) work at Premera are required to report family relationships to management and Employee Experience when they change jobs, change job responsibilities, transfer internally, have a change in leadership, or have any change to their employment situation in which their family relationship may create any actual or perceived conflict of interest.

Conflicts of interest

Outside activities

We must also avoid other employment or activities that affect our jobs at Premera. This includes anything that could negatively affect the following:

- Work hours, job responsibilities, or quality of work
- Obligations to Premera

Employees must disclose to their manager and Regulatory Compliance & Ethics all outside employment.

Medical professionals employed at Premera are expected to clearly understand their roles and responsibilities while working on behalf of Premera, especially if their work here excludes actions that would normally be taken in a clinical practice. Unless otherwise stated in the scope of work performed for Premera, medical professionals at Premera are not to treat, prescribe treatment, or render prescriptions to other employees, non-employees, or customers while working on behalf of Premera.

Q: I have a side business that sometimes requires I make personal phone calls during Premera work hours. Is that okay as long as my work is getting done?

A: No, you should not be using Premera property or your work time at Premera for a side business.

Personal financial gain

Employees must not own or have a significant financial interest in a company that does business with or competes with Premera. We also should not use our position to influence any decisions we have a vested interest in and should disqualify ourselves from any decisions where we may be directly or indirectly impacted personally. We must avoid activities or actions that might influence or appear to influence our jobs at Premera. The chart below contains examples of potential conflicts and what should and shouldn't be disclosed.

SITUATION	NEED TO DISCLOSE?
Applying for a position in Claims and your sister-in-law is one of the team leads	**Disclose**
Have a second job at Macy's	**Disclose**
Neighbor works at Regence	**Don't Disclose** (but don't share confidential and proprietary information)
Significant other is a board member for PalAmerican (third-party physical security)	**Disclose**
Cousin works at Kaiser Permanente but I never talk to him	**Disclose**
Best friend works at Providence	**Don't Disclose** (but don't share confidential and proprietary information)

Corporate opportunities

You must not profit from opportunities that are discovered through your job at Premera. This includes the use of Premera property or confidential information for personal gain or for competing with Premera.

Conflicts of interest

Intellectual property

All intellectual property used, created, or developed within the scope of an employees' employment, whether alone, or with other Premera employees, continues to belong to Premera. This includes, among other things, work-related ideas, concepts, algorithms, innovations, inventions, discoveries, copyright protected works, source code, trade secrets, know-how, and confidential information.

However, employees will retain ownership of intellectual property, including inventions developed entirely on their own time and without use of Premera's equipment, supplies, facilities, or trade secret information, unless the invention relates directly to the business of the employer, or to the employer's actual or demonstrably anticipated research or development, or the invention results from any work performed by the employee for Premera. See **Appendix C** for links to applicable Washington laws regarding the assignment of employees' rights to invention.

Q: I am a database developer and while working on a Premera project, I came up with an idea for a new health database that I'd like to sell. Since this is my design, can I do that?

A: No, you cannot sell something you created while employed at Premera if it is related to the work you do here.

Kickbacks and rebates

Employees and their family members may not receive personal kickbacks or rebates as a result of purchasing or selling goods and services for Premera. Kickbacks and rebates can take many forms and are not limited to direct cash payments or credits. Generally, if an employee or family member might gain personally through the transaction, it is prohibited. Such practices are unethical and may be illegal. Contact a manager or Regulatory Compliance & Ethics with questions about a transaction.

Q: My brother-in-law owns a restaurant and I often buy gift certificates from him to give to Premera employees and clients. In exchange, he sometimes buys me dinner. Is this okay?

A: No, a kickback is anything received from a third party for sending business their way. This could include gift cards, dinner, or other types of perks. You should not accept gifts from your brother-in-law, and you should also disclose this relationship on your Conflict of Interest survey.

Bribery, corruption, and improper payments

We do not directly or indirectly solicit, accept, offer, promise, authorize, or give bribes or other improper payment to or from anyone. This includes facilitation payments. No payment or benefits, other than those approved by Premera, may be made to customers or prospective customers as an incentive to buy our products. Using Premera funds or assets for any unlawful or unethical purpose is prohibited. Remember, Do the Right Thing.

Payments to producers, representatives, and consultants

All agreements with producers, sales representatives, third parties, and non-employees must be in writing and approved by Legal or Enterprise Vendor Management and Contracting. The agreement must clearly and accurately define the services to be performed and the commission or fee involved. Any payments must be reasonable in amount and priced fairly for the value of the services rendered. Refer to our Third Party Code for more information.

Conflicts of interest

Gifts and gratuities

Even the mere appearance of impropriety in giving or receiving gifts, entertainment, or things of value can jeopardize the company's interests, and is inconsistent with Premera's commitment to the highest level of integrity. Gifts should not be solicited from our customers, third parties, or business partners. Employees may not—under any circumstance–accept gifts of cash from these parties.

Employees and family members may accept unsolicited, non-cash gifts from a third party or business partner, or potential third party or business partner if the gift is small in value. A useful guideline is that gifts under $75 are normally considered nominal. Regulatory Compliance & Ethics should approve acceptance of all gifts that are not promotional in nature, such as tickets to sporting and entertainment events, gift cards, meal certificates, and bottles of alcohol.

Gifts or entertainment must be provided in an honest and transparent manner. They must be designed to avoid any actual or perceived influence and must be appropriate to the occasion and to the position of the third party and the recipient. Below are some examples of when it is and isn't appropriate to accept gifts from third parties and business partners, or potential third parties and business partners:

USUALLY OKAY TO ACCEPT:	USUALLY NOT OKAY TO ACCEPT:
$200 gift card won during a random drawing at a business conference	Cash for dinner
$75 ticket to a sporting event	$100 ticket to a sporting event
$10 Starbucks gift card from a third party	$10 Starbucks gift card from a government employee
Birthday gift from your mother who is a contracted provider	$100 bottle of wine
Dinner at a business conference	Travel expenses to the business conference
Lunch with a non-employee worker to discuss service levels	Lunch for you and your spouse without the third party

Q: A third party I work with offered me two tickets to a sporting event. Can I accept these?

A: It depends. First find out how much the tickets cost. If each ticket is $50, then you could accept one, but not both. Generally, you can accept a non-cash gift if the value of the gift is under $75 and is not intended to influence you.

Leaders should use appropriate judgment when providing rewards or recognition to their team. Recognition may be demonstrated by providing some forms of entertainment or gifts, which must be professional and of appropriate value for the situation. If alcohol is provided, consideration should be given to whether the participants are comfortable with this type of reward. When providing alcohol at a Premera event, please refer to the Alcohol, Drug, and Substance Use policy and Limited Alcohol Use Guidelines.

Additionally, any event where Premera employees or customers are present, whether organized or casually arranged, must demonstrate inclusivity to all employees regardless of race, color, ethnicity, national origin, sex, gender identity and expression, marital status, age, sexual orientation, disability, language fluency, religion, genetic information, and veteran status.

Conflicts of interest

Entertainment

Gifts, entertainment, and other things of value are often intended to build relationships. However, gifts and entertainment that appear to compromise an employee's ability to make fair business decisions create ethical issues. Employees may offer or accept entertainment from a Premera third party or business partner. For example, it's okay to accept an invitation to dinner or to join a third party or business partner at a sporting event. We generally are allowed to attend such events with existing vendors and partners, but not with potential companies trying to win our business. If the entertainment is primarily intended to gain favor, it is not allowed. For example, accepting a gift of entertainment tickets to enjoy on one's own, without the company of a third party or business partner, is not allowed. Before accepting or offering entertainment, employees should obtain their manager's approval. Managers should contact Regulatory Compliance & Ethics with any questions about the appropriateness of the entertainment. When accepting or providing offers of entertainment on behalf of Premera, **all employees are expected to model appropriate behavior and Do the Right Thing.**

Workplace conduct

“Our purpose comes to life by living our values.”

— Cecily Hall, EVP, Employee Experience

Workplace conduct

Workplace conduct and employment practices

Premera's Employee Experience department is responsible for overseeing Premera's procedures for the hiring, promotion, compensation, corrective action, and employment termination of employees. It is your responsibility to read, understand, and comply with Employee Experience's established policies and guidelines. For more guidance, consult with your manager, your Employee Experience representative, or the policies and guidelines issued by Employee Experience.

Safety, health, and environment

We are committed to providing a safe and healthy workplace for employees and for visitors to our campuses. We are equally committed to minimizing the environmental impact of our operations. These commitments can only be met through awareness and cooperation. Each of us is responsible for helping to maintain a safe and healthy work environment.

Visit the Real Estate & Facilities internal website for additional information on how to request maintenance and/or repairs, and to report safety and security issues. Visit the Worker's Compensation internal website for more information on what to do in case of a workplace incident.

Q: A co-worker just emailed me an inappropriate joke. What should I do?

A: Let the employee know it made you feel uncomfortable, or talk to your manager.

Q: Susie is always telling jokes about religion and I don't like it, but what can I do?

A: Let Susie know that it is not appropriate to tell jokes about religion. If you are not comfortable doing that, talk to your manager, contact Regulatory Compliance & Ethics or Employee Experience, or call the Compliance & Ethics Hotline.

Q: I got injured while working on campus. Should I tell someone?

A: Tell your manager or a member of Premera's Safety Committee. You also need to complete an Incident Report Form, which can be found on the Worker's Compensation internal website.

Reporting suspected noncompliance

"Our Regulatory Compliance & Ethics team is your partner. Please contact us with anything you want to discuss. We'd love to hear from you!"

— Sven Peterson, Corporate Compliance and Ethics Officer

Reporting suspected noncompliance

Reporting violations and seeking guidance

We all must work together to help protect Premera from actions that could harm our operations, reputation, or future growth. All employees are therefore expected to report actual or suspected violations involving the following:

- This Code of Conduct
- Corporate and departmental policies
- Laws or regulations
- Third-party Codes of Conduct

Any employee who suspects violations should talk to a manager, Regulatory Compliance & Ethics, or Employee Experience. We value the right for employees to remain anonymous. Employees are encouraged to contact the Compliance & Ethics Hotline, our third-party-managed hotline or MyComplianceReport.com, 24 hours a day, 7 days a week. Reports may be made anonymously and confidentially, if desired. Confidentiality is maintained to the extent permissible by law and deemed appropriate for the situation. Remember, we have a policy that prohibits retaliation and intimidation for a good faith report. Premera fully supports whistleblower protection laws.

Anyone choosing to report anonymously should include as many details as possible. We may not be able to complete our investigation if we do not have adequate information. Also, check back frequently to ensure additional information is not needed.

Managers who receive a possible violation report from an employee must have it investigated. Managers who do not feel they have the expertise to research and resolve the issue should contact Regulatory Compliance & Ethics or Employee Experience. Each incident must be thoroughly investigated, and corrective actions must be taken if necessary.

Conducting investigations

When an incident is reported, it may be investigated by Regulatory Compliance & Ethics, Employee Experience, Internal Audit, Legal, Privacy, or the Special Investigations Unit.

Investigation details and identities are confidential to the extent permissible by law and deemed appropriate for the situation.

Reporting suspected noncompliance

Corrective action

When a reported violation is confirmed, we will implement corrective action.

Please note that if an incident is reported, the person who reported it may not be informed of the outcome. This is to protect the confidentiality of those involved in the investigation.

We take our Code of Conduct seriously. Violations of the Code or our policies may be grounds for corrective action, up to and including termination of employment.

Examples of when corrective actions may be taken include:

- Participation in or authorization of actions that violate this Code
- Failure to report a violation
- Refusal to cooperate in an investigation, providing false or misleading information, or withholding information that may be deemed pertinent to the investigation
- Failure of a manager to detect and report a violation, if the failure reflects grossly inadequate supervision
- Retaliation and/or intimidation against an employee who reports a potential violation or participates in an investigation in good faith

Employees are encouraged to self-report a violation, which will be considered when determining corrective action. Intentional cover-up of violations is prohibited.

Q: I saw something that I think is against corporate or departmental policy, but I'm not sure of all the facts. I don't want to report something inaccurately and get someone in trouble. What should I do?

A: You can discuss the situation with your manager, Employee Experience, Regulatory Compliance & Ethics, or you can report your concern using the Compliance & Ethics Hotline. If you choose to report anonymously, please check back frequently to ensure additional information is not needed.

Q: I reported a concern via the Compliance & Ethics Hotline and I'm not sure what the outcome was. Why should I report concerns in the future?

A: All items reported via the Compliance & Ethics Hotline, or directly to Employee Experience or Regulatory Compliance & Ethics, are thoroughly investigated. There are several reasons it may appear that nothing happened: 1) not enough details were submitted to conduct a thorough investigation; 2) no wrongdoing was discovered after the investigation was complete; or 3) corrective action occurred but could not be publicized to protect all parties involved with the investigation. If the situation occurs again, or continues to occur, report it again and include as many specific details as possible.

Appendix A:

Major federal laws regarding federal and federal-supported healthcare programs applicable to Premera

Anti-Kickback Statute – 42 United States Code (U.S.C.), Sec. 1320a-7b(b) and Safe Harbor regulations – 42 CFR, Sec. 1001.952; for more information, visit **https://oig.hhs.gov/compliance/safe-harbor-regulations**.

Civil Monetary Penalties (CMPs) – 42 U.S.C., Sec. 1320a-7a.

Criminal Health Care Fraud Statute – 18 U.S.C., Sec. 1347.

Employee Retirement Income Security Act of 1974 (P.L. 93-406).

Exclusions – 42 U.S.C., Sec. 1320a-7; 42 U.S.C., Sec. 1395(e)(1) and Sec. 1395w-27(g)(1)(G); 42 CFR, Sec. 1001.1901.

False Claims Act (FCA) – 31 U.S.C., Sec. 3729-3733 and 18 U.S.C., Sec. 287; for more information, visit **https://oig.hhs.gov/fraud**.

HIPAA – Act of 1996 (P.L. 104-191); 45 CFR Part 160 and Part 164, Subparts A and E.

Internal Revenue Code of 1986.

Patient Protection and Affordable Care Act (P.L. 111-148) including the amendments made by the Health Care and Education Reconciliation Act of 2010 (P.L. 111-152).

Physician Self-Referral Law (Stark Law) – 42 U.S.C., Sec. 1395nn; for more information, visit **www.cms.gov/Medicare/Fraud-and-Abuse/PhysicianSelfReferral** on the CMS website.

Public Health Service Act (P.L. 78-410).

Social Security Act – Title XVIII.

Appendix B:

Definitions and key indicators of potential fraud, waste, and abuse (FWA)

Potential fraud, waste, and abuse (FWA) events and activities related to external parties:

- **Fraud**: Intentionally submitting false information in order to get money or a benefit.
- **Waste and Abuse**: Requesting payment for items and services when there is no legal entitlement to payment. Unlike fraud, the provider might not have knowingly and/or intentionally misrepresented facts to obtain payment.

Beneficiary:

- Does the prescription look altered or possibly forged?
- Have you filled numerous identical prescriptions for this beneficiary, possibly from different doctors?
- Is the person receiving the service or picking up the prescription the actual beneficiary (identity theft)?
- Is the prescription appropriate based on the beneficiary's other prescriptions?
- Does the beneficiary's medical history support the services being requested?

Provider:

- Does the provider write for diverse drugs or primarily only for controlled substances?
- Are the provider's prescriptions appropriate for the member's health condition (medically necessary)?
- Is the provider writing for a higher quantity than medically necessary for the condition?
- Is the provider performing unnecessary services for the member?
- Is the provider's diagnosis for the member supported in the medical record?
- Does the provider bill the sponsor for services not provided?

Pharmacy:

- Are the dispensed drugs expired, fake, diluted, or illegal?
- Do you see prescriptions being altered (changing quantities or Dispense As Written)?
- Are proper provisions made if the entire prescription cannot be filled (no additional dispensing fees for split prescriptions)?
- Are generics provided when the prescription requires that brand be dispensed?
- Are pharmacy benefit managers (PBMs) being billed for prescriptions that are not filled or picked up?
- Are drugs being diverted (drugs meant for places such as nursing homes or hospice being sent elsewhere)?

Appendix B

Definitions and key indicators of potential fraud, waste, and abuse (FWA), continued

Wholesaler:

- Is the wholesaler distributing fake, diluted, expired, or illegally imported drugs?
- Is the wholesaler diverting drugs meant for nursing homes, hospices, and AIDS clinics and then marking up the prices and sending to other smaller wholesalers or to pharmacies?

Manufacturer:

- Does the manufacturer promote off-label drug usage?
- Does the manufacturer provide samples, knowing that the samples will be billed to a federal healthcare program?

Plan sponsor:

- Does the sponsor offer cash inducements for beneficiaries to join the plan?
- Does the sponsor lead the beneficiary to believe that the cost of benefits are one price, when the actual costs are higher?
- Does the sponsor use unlicensed agents?
- Does the sponsor encourage or support inappropriate risk adjustment submissions?

Potential fraudulent activity committed by employees, including officers, and non-employees:

- Assets—means equipment, company property and buildings, inventory, corporate funds, supplies, concepts, business strategies and plans, financial data, records and work files, employees' work time, intellectual property, and other confidential information about the business and our customers.
- Fraud—means the intentional, false representation or concealment of material fact(s) or information.

Examples of fraud and key indicators may include, but are not limited to:

- Forgery or intentional alteration of a check, bank draft, or other financial document belonging to or issued by the company.
- Falsification of claims, time sheets, expense reports, financial or other business reporting documents, or employment records or reports.
- Anomalies in documents and financial statements.
- Unusual situations or reports involving unexpected amounts, frequencies, people, places, and times.
- Misappropriation of funds, securities, supplies or other assets.
- Intentional mishandling or misreporting of money or financial transactions.
- Preparation of intentionally misleading or false financial statements.

Appendix C

Washington revised code § 49.44.140 (requiring assignment of employees' rights to inventions—conditions)

(1) A provision in an employment agreement which provides that an employee shall assign or offer to assign any of the employee's rights in an invention to the employer does not apply to an invention for which no equipment, supplies, facilities, or trade secret information of the employer was used and which was developed entirely on the employee's own time, unless (a) the invention relates (i) directly to the business of the employer, or (ii) to the employer's actual or demonstrably anticipated research or development, or (b) the invention results from any work performed by the employee for the employer. Any provision which purports to apply to such an invention is to that extent against the public policy of this state and is to that extent void and unenforceable.

(2) An employer shall not require a provision made void and unenforceable by subsection (1) of this section as a condition of employment or continuing employment.

(3) If an employment agreement entered into after September 1, 1979, contains a provision requiring the employee to assign any of the employee's rights in any invention to the employer, the employer must also, at the time the agreement is made, provide a written notification to the employee that the agreement does not apply to an invention for which no equipment, supplies, facility, or trade secret information of the employer was used and which was developed entirely on the employee's own time, unless (a) the invention relates (i) directly to the business of the employer, or (ii) to the employer's actual or demonstrably anticipated research or development, or (b) the invention results from any work performed by the employee for the employer.

PREMERA | BLUE CROSS BLUE SHIELD OF ALASKA

An Independent Licensee of the Blue Cross Blue Shield Association

034215 (04-21-2025)