PREMERA | BLUE CROSS

VENDOR GUIDELINES

Guidelines for vendors working with Premera Blue Cross

Premera Blue Cross is committed to complying with the letter and spirit of all applicable legal and ethical standards with the highest degree of integrity and honesty.

General Expectations

Adopt a code of ethical behavior and comply with all applicable laws and regulations
Inform Premera of major organizational changes (such as a merger or acquisition), changes in the account team, or operations that may affect the services or service levels
Notify Premera in advance and obtain permission prior to engaging any subcontractors or offshoring any service operations
Avoid offering favors, gifts, or gratuities to Premera associates that may appear to create a conflict of interest
Adopt written policies and procedures that provide protections for employees who report suspected fraud, waste, and abuse
Maintain all records pertaining to the services for up to 10 years based on Premera and regulatory requirements

Security Guidelines

Premera will conduct initial and periodic vendor risk assessment based on the nature of services provided and type of information accessed
Vendors must conduct background and OIG sanction checks on all employees, subcontractors, and agents who provide services or who have access to Premera information
Vendors with access to Premera protected health information (PHI), personal protected information (PPI), or private company information must: » Have a fully executed non-disclosure agreement, contract and Business Associate Agreement (BAA) prior to data exchange » Comply with all federal and state data privacy laws, including HIPAA and HITECH » Undergo a periodic Vendor security assessment conducted by Premera or its security assessment delegate » Provide Premera audits of its internal controls (e.g. SOC2 Type 2, SOC1 Type 2, HITRUST) » Provide evidence of security controls in the form of vulnerability and penetration testing (network, host, application)

» Ensure compliance with security controls with supporting policies & procedures
» Agree to notify Premera promptly in the case of a security or data breach
» Ensure proper handling and disposal of corporate proprietary information, PHI, and PPI

Payment

Premera requires a fully executed contract and purchase order to pay vendor invoices

Legal and Regulatory

All vendors must be cleared through the Office of Inspector General, the Office of Foreign Assets Control, and the System for Award Management, Excluded Party List System sanction checks

Vendors who are a Centers for Medicare & Medicaid (CMS) first-tier, downstream, or related entity (FDR) must also conduct monthly sanction checks on their employees and vendors and at time of hire/contracting

If designated as an FDR, the vendor must comply with CMS regulations, including but not limited to annual CMS compliance and fraud, waste, and abuse training and certification for their employees and vendors

Risk and Audit

Vendors are expected to carry appropriate insurance and provide evidence of coverage

Premera reserves the right to conduct a periodic audit and review of all records related to services rendered under the agreement or contract

Vendors must accept unlimited liability for breaches of confidential information

Financial Viability

Provide written evidence of financial viability, which may include audited financial statements

Anti-Discrimination and Social Responsibility

Premera encourages vendors to adopt environmental sustainability policies

Vendors must agree not to discriminate in employment on the basis of sex, age, race, color, religion, origin, sexual orientation, gender identity or expression, health status, or disability

Disaster Readiness and Business Continuity

Provide evidence that a disaster readiness or business continuity plan is in place to ensure supply of product or service in the event of business disruption

Records

Vendors must maintain accurate records with respect to services provided to Premera and follow the Premera records retention schedule