MASSACHUSETTS

Vendor Guidelines

Guidelines for Vendors Working with Blue Cross Blue Shield of Massachusetts

Blue Cross Blue Shield of Massachusetts' code of conduct states that Blue Cross and its Board of Directors, management, and associates are 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 conduct, and comply with all applicable laws and regulations
- Inform Blue Cross 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 expected under contract
- Notify Blue Cross and obtain its permission prior to engaging subcontractors or offshoring that may affect services under contract
- Avoid offering favors, gifts, or gratuities to Blue Cross 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

Security Guidelines

- Blue Cross will conduct initial and periodic vendor risk assessments based on the nature of services provided and type of information access
- Vendors must conduct background checks on all employees and other workers or agents who provide onsite services or who have access to Blue Cross information
- Vendors with access to Blue Cross PHI (protected health information), PI (personal information), or private company information must:
  - Have a fully executed non-disclosure agreement or a contract that includes Blue Cross confidentiality terms before data is exchanged
  - Comply with all applicable federal and state data privacy laws, including HIPAA, HITECH, and Mass ID theft
  - Undergo a periodic risk assessment or audit of controls by a third party of its general IT controls (e.g., SSAE 16 SOC1 or SOC2 audit, HITRUST certification)
  - Provide evidence of security controls in the form of vulnerability and penetration testing (network, host, application)
  - Ensure compliance with security controls with supporting policies and procedures
  - Agree to notify Blue Cross in the case of a security or data breach
  - Ensure proper handling and disposal of Blue Cross corporate private information, PHI, and PI
  - Encrypt all PHI at-rest in your environment compliant with HIPAA guidelines

continued

Blue Cross Blue Shield of Massachusetts is an Independent Licensee of the Blue Cross and Blue Shield Association

Payment

- Blue Cross 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 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
- Blue Cross reserves the right to conduct a periodic audit and review of all records related to contracted services
- Vendors must accept unlimited liability for their breaches of confidential information, gross negligence, and willful acts; this also applies to their subcontractors

Financial Viability

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

Diversity and Social Responsibility

- Blue Cross encourages vendors to adopt diversity and inclusion policies
- Blue Cross 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 Blue Cross and follow the Blue Cross records retention schedule
- Maintain all records pertaining to Blue Cross Medicare Parts C and D business for 10 years

For more information

If you have any questions, please contact our Compliance Helpline at 1-877-874-8416.

MASSACHUSETTS

® Registered Marks of the Blue Cross and Blue Shield Association. © 2017 Blue Cross and Blue Shield of Massachusetts, Inc., and Blue Cross and Blue Shield of Massachusetts HMO Blue, Inc.

178453M

55-1731 (10/17)