# Responsible Business

- Ethical and responsible business conduct
- Human rights
- Data privacy and information security
- Supply chain management
- Economic performance
- Indirect economic impacts
- Tax strategy

eHealth's commitment to our customers, our employees, and our stakeholders goes beyond the mission of connecting consumers with the right insurance coverage. We connect them safely and ethically. One of the signs of our success in delivering superior customer experience is our 4.6 out of 5-star Trustpilot consumer rating as of August 2024 for eHealth Medicare.

We also set high standards for the insurers whose plans we offer. eHealth stands out among our competitors because of the large choice of health insurance plans we carry on our platform, but we only partner with those insurance carriers who pass our vetting process. We also carefully review our plan selection to ensure we offer quality insurance products that benefit our customers. Our practice is to market plans using transparent messaging and in compliance with relevant laws and regulations. Protecting the privacy and security of our customers' data is crucial for delivering on our mission, and we have a broad program of safeguards, audits, and employee training in place to do just that. Our practices are rooted in globally recognized standards and third-party certifications to assure our customers that their information is secure with us.

## Governance

Good governance is essential for managing a business successfully. It serves as the foundation for leading and directing the company. It is our Board of Directors that has ultimate oversight over eHealth's business strategy. Together, the Board and its committees ensure safeguards and management policies are in place to maintain business continuity and succeed in an ever-changing business environment. The Board and its Compensation Committee also annually review the performance of our executive officers in connection with the determination of the salary and other compensation of our executive officers (including the Chief Executive Officer). The Chief Executive Officer reviews succession planning and management development with the Board on a regular basis.

The members of our Board of Directors represent the diverse perspectives needed to steer a company in an ever-changing business environment. The Board currently is made up of nine members and has always included a majority of independent directors (8 out of 9). A matrix showing the diversity of our Board of Directors, as self-disclosed by our directors, is as follows:

### Responsible Business Relevant SDGs

8 DECENT WORK AND ECONOMIC GROWTH

9 INDUSTRY, INNOVATION AND INFRASTRUCTURE

10 REDUCED INEQUALITIES

11 SUSTAINABLE CITIES AND COMMUNITIES

16 PEACE, JUSTICE AND STRONG INSTITUTIONS

**Board Diversity Matrix** (as of September 24, 2024)

| Total Number of Directors | | | 8 | |
|---|---|---|---|---|
| | Female | Male | Non-Binary | Did not Disclose Gender |
| **Part I: Gender Identity** | | | | |
| Directors | 4 | 4 | — | 1 |
| **Part II: Demographic Background** | | | | |
| African American or Black | — | — | — | — |
| Alaskan Native or Native American | — | — | — | — |
| Asian | 1 | — | — | — |
| Hispanic or Latinx | — | — | — | — |
| Native Hawaiian or Pacific Islander | — | — | — | — |
| White | 3 | 3 | — | — |
| Two or More Races or Ethnicities | — | 1 | — | — |
| LGBTQ+ | | | 1 | |
| Did not Disclose Demographic Background | | | 1 | |

The standing committees of the Board are the Audit Committee, the Compensation Committee, the Nominating and Corporate Governance Committee, and the Government and Regulatory Affairs Committee. Interested parties can learn more about the individual members and committees of our Board on our Investor Relations website under the Governance section.

## Risk Management

The Board of Directors takes an active role, as a whole and at the committee level, in overseeing management of the company's risks and through its Audit Committee. The Audit Committee is responsible for reviewing the Company's Enterprise Risk Management (ERM) program in consultation with eHealth's management and our independent auditors. In addition, strategic risks are overseen by the full Board of Directors; regulatory risks are overseen by the Government and Regulatory Affairs Committee; financial and cybersecurity risks are overseen by the Audit Committee; risks relating to compensation plans and arrangements are overseen by the Compensation Committee; and risks associated with director independence and potential conflicts of interest are overseen by the Nominating and Corporate Governance Committee.

Our senior leadership team is closely involved, and our management keeps the Board apprised periodically of significant risks facing the company and the approach being taken to understand, manage, and mitigate those risks. Additional review or reporting on enterprise risks is conducted as needed or as requested by the full Board of Directors or the appropriate committee. Our chairperson of the Board promotes communication and consideration of matters presenting significant risks to us through their role in contributing to agendas for meetings of our Board and acting as a conduit between our independent directors and our Chief Executive Officer on sensitive issues.

## Ethical and Responsible Business Conduct

We are committed to honest and ethical conduct as outlined in our various corporate governance policies, including, the Code of Business Conduct, Anti-Corruption and Anti-Bribery Policy, Insider Trading Policy, Regulation FD Corporate Communications Policy, Related Person Transaction Policy and Whistleblower Policy. These policies include broad principles in relation to ethical and responsible behavior, including conflicts of interest, legal compliance and reporting, which all employees are trained in at point of hire and through periodic mandatory training, including annual acknowledgment of these policies.

## Responsible Product Offering

As of December 31, 2023, eHealth's Compliance Department had 43 people with a departmental mandate of making sure the company remains in compliance with Centers for Medicare & Medicaid Services (CMS), state departments of insurance and other applicable regulations as well as rules from our carrier partners. The Compliance Department is led by eHealth's Vice President Compliance, Chief Medicare Compliance Officer who reports to our General Counsel. eHealth's Medicare compliance program is overseen by the company's Medicare Compliance Committee.

The Compliance Committee meets at least four times per year or more frequently as necessary. The Committee's responsibilities include but are not limited to:

- Overseeing the Medicare Compliance Program.
- Updating the Compliance Program as well as written policies and procedures that promote and pertain to compliance.
- Reviewing and approving regular, effective education and training programs addressing compliance issues and responsibilities.
- Developing a system for confidential reporting of instances of noncompliance and investigating and responding to these reports.
- Developing protocols for consistent enforcement of appropriate disciplinary action against persons who have engaged in acts or omissions constituting non-compliance.
- Assisting with the development and implementation of risk assessment associated with eHealth Medicare operations and the use of audits, investigations and other evaluation techniques to assess the effectiveness of compliance corrective measures.

**Membership of the Medicare Compliance Committee consists of individuals with decision-making authority and/or in-depth knowledge in their respective areas of expertise from the following areas:**

- Compliance
- Human Resources
- Sales/Customer Care
- Medicare Operations
- Product Management
- Carrier Relations
- Marketing
- Legal

eHealth continues to receive positive feedback from carriers with respect to the significant progress we've achieved in driving our enrollment quality and CTM scores since the initiation of our business transformation in 2022.

eHealth's employees are also required to participate in Medicare Compliance Program, FWA, privacy, Information Security, corporate governance, Code of Business Conduct, Harassment and Discrimination Prevention, and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) training shortly after commencing employment and annually thereafter. eHealth's licensed insurance agents, or benefit advisors, are required to participate in these trainings as well as additional training sessions in order to qualify to sell Medicare plans.

Beyond these training mandates, the company also internally tracks a host of metrics that are indicative of customer satisfaction, including but not limited to, our plan retention rates and Complaint Tracking Module (CTM) scores. The CTM tracks beneficiary complaints filed directly with the CMS. eHealth continues to receive positive feedback from carriers with respect to the significant progress we've achieved in driving our enrollment quality and CTM scores since the initiation of our business transformation in 2022.

On a quarterly basis, eHealth publishes updates to our lifetime value estimates for each of our commission-based products. We believe lifetime value is one of several ways to gauge long-term customer satisfaction as it is influenced by the amount of time a beneficiary remains enrolled in a specific plan. It is in the combined interest of the beneficiary, eHealth, and the carrier to create long-lasting enrollments. Because of this, eHealth goes above and beyond the requirements of CMS and our carrier partners in our goal of creating high quality and long-lasting enrollments. One of these actions includes a verification step at the end of each enrollment call where a second agent reviews the plan with the beneficiary. We are also pursuing additional services to impact lifetime value estimates. These include finding primary care practitioners for our beneficiaries, scheduling initial provider appointments, conducting health risk assessments (HRAs), activating covered benefits, as well as other services, with the goal of helping members get the most of their coverage.

eHealth also maintains an Investigation, Remediation and Disciplinary Standards policy. The policy guides the company's processes for promptly responding to compliance concerns as they are identified or reported, conducting a thorough and documented investigation of reported concerns, as well as identifying compliance concerns through the course of routine monitoring and audits. The Policy also addresses correcting confirmed compliance violations promptly and thoroughly to reduce the potential for recurrence and to promote ongoing compliance with CMS requirements. Additionally, the policy guides eHealth's disciplinary standards to remediate confirmed compliance violations. The procedures described under eHealth's Investigation, Remediation, and Disciplinary Standards policy are below:

### 1. Investigation

a. eHealth conducts timely, reasonable inquiries into any conduct where evidence suggests there has been misconduct related to services performed under the MA and the Medicare Part D contract and supply such research to applicable Medicare Advantage Organizations and Prescription Drug Plan Sponsors ("Carriers") with which eHealth contracts for further investigation and corrective action.

b. The Chief Compliance Officer or their designee initiates a reasonable inquiry immediately, but no later than two (2) days from the date the potential misconduct is identified.

c. A reasonable inquiry will include a preliminary investigation of the matter by the Chief Compliance Officer or their designee.

d. Based on the outcome of the investigation, eHealth will implement appropriate corrective actions, up to and including termination (for example: disciplinary actions against responsible individual(s)) in response to a confirmed violation.

### 2. Remediation

a. The Chief Compliance Officer or their designee designs any corrective action plan to be tailored to the determined root cause of the misconduct and to address the particular misconduct identified.

b. All corrective action plans will indicate timeframes. When developing corrective actions for misconduct by a Downstream Entity, the elements of the corrective action may be detailed in a written agreement with the entity. These elements include all ramifications should the subcontractor fail to satisfactorily implement the corrective action(s).

c. The elements of the corrective action plan that address misconduct committed by employees will be documented and include disciplinary actions should employee(s) fail to satisfactorily implement the corrective actions.

d. Corrective actions will be evaluated upon implementation and may continue to be monitored after implementation to validate effectiveness.

### 3. Disciplinary Actions

a. When a compliance investigation results in the need to consider individual disciplinary actions, eHealth's Compliance will consult with Human Resources (HR) the individual's manager, and on an as-needed basis, Legal. eHealth's HR Department retains records of all disciplinary actions taken to address confirmed compliance violations. These records include, but are not limited to, the following information:

   i. The date the violation was reported;

   ii. A description of the violation;

   iii. The date of the investigation;

   iv. A summary of the findings;

   v. Any disciplinary action taken and the date it was taken.

b. To promote consistency and fairness in relation to agent disciplinary action, eHealth has established an Agent Oversight and Terminations Committee, serving as a subcommittee to the Medicare Compliance Committee. In addition, HR periodically reviews records of discipline for compliance violations.

### 4. Reporting

a. As appropriate, eHealth will forward potential cases of FWA and noncompliance to the Carrier to allow for investigation and self-reporting as required to CMS, the MEDIC, OIG and/or other law enforcement entities.

**5. Dissemination of Disciplinary Standards**

a. The eHealth Medicare Compliance and FWA training module outlines the expectations for all employees, governing body members, and downstream entities to report compliance concerns and cooperate and assist in the resolution of any reported non-compliance issue. Additionally, the Code of Business Conduct further defines eHealth's commitment to ethical business practices and compliance, emphasizing the importance of reporting compliance concerns and the disciplinary actions that may result from confirmed compliance violations.

b. To further encourage the reporting of compliance-related issues, eHealth may use one of the following methods to publicize how to report the issue and what the potential disciplinary guidelines would be in a case of non-compliance:

   i. Newsletters and/or Bulletins which explain compliance issues and methods;

   ii. Regular presentations at department staff meetings;

   iii. General compliance training;

   iv. Job specific training;

   v. Compliance Department website; and

   vi. Prominently displayed posters or other such vehicles that emphasize the importance of compliance.

## Human Rights & Key Stakeholders

eHealth supports worker rights by ensuring that fair wages, benefits, decent working conditions, and overall human rights are respected across our global workforce. Terms are specified within our Code of Business Conduct and Employee Handbook. In addition, we adopted the Global Human Rights Policy and the Vendor Code of Conduct in June 2021, in which we communicate our commitments and expectations to our vendor base, and reflect values and policies included in specific human rights conventions, such as the United Nations Universal Declaration on Human Rights, International Labor Organization Conventions, and the Organization for Economic Co-operation and Development's Guidelines for Multinational Enterprises.

At eHealth, we partner with a large network of approximately 180 reputable insurance carriers to ensure our customers have access to a broad choice of quality Medicare, individual and family, small business, and ancillary health insurance plans. We are uniquely positioned between consumers and carriers as a technology-powered marketplace. Our multi-channel marketing organization communicates our value proposition to consumers and drives visits to our online platforms and calls to the licensed agents at our customer care centers. Our Human Resources team assists in attracting and cultivating talent, while our legal department ensures that we maintain our strong track record of compliance with federal, state, and local regulations in the insurance industry. Our internal product and technology team, consultants, and third-party information technology service providers help us offer industry-leading technological capabilities while at the same time remaining vigilant in the areas of data security and privacy.

We are committed to working with the leading carriers in the country and before adding any carrier to our platform, we conduct a vetting process. Factors we consider include AM Best ratings of financial stability, quality of customer service, product offerings, and rate stability. We also closely monitor performance and adherence to best practices and conduct detailed business reviews with our leading carriers on a regular basis. In our largest business segment, Medicare, plan quality and performance metrics are guided and controlled by CMS. State departments of insurance also have the power to provide standards that plans are required to meet in order to be offered.

Our culture is one that focuses on nurturing relationships. Therefore, we work closely with our supply chain partners to correct problems and strengthen efforts so that we can reduce risks and achieve our shared objectives.

## Data Privacy and Information Security

Managing privacy and information security risks is particularly important for our company. We are committed to maintaining information security through responsible management, appropriate use, and protection in accordance with legal and regulatory requirements and our agreements. This is an integral part of our organization, and eHealth employees understand that information security is everyone's responsibility.

We value the trust our customers and business partners place in us to protect their sensitive information. We maintain data privacy and security through a robust program of safeguards, including responsible management, appropriate use, and protection of data in accordance with legal and regulatory requirements. Early on, we identified information security as a salient risk as described in our filings with the Securities and Exchange Commission. We also have an established Privacy Policy, which applies to all eHealth operations.

eHealth maintains an Information Security team, focusing on information and systems technology, corporate governance, and behaviors to drive security best practices and safeguard information from unauthorized or inappropriate access, use, or disclosure.

eHealth also has a Privacy Officer who advises the company on privacy related laws and regulations, provides guidance on privacy compliance, drives privacy policy, creates and delivers privacy training across the organization, and oversees the privacy program. eHealth's Board of Directors has ultimate oversight over our privacy, information security, governance, risk management and compliance programs and strategies.

The Board executes this oversight both directly and through its Audit Committee. Together, the Board and the Audit Committee ensure that eHealth has privacy and information protection management policies and processes in place. The Audit Committee is regularly briefed on issues related to eHealth's risk profile. These briefings are designed to provide visibility about the identification, assessment, and management of critical risks, audit findings, and management's risk mitigation strategies. Management briefs the Audit Committee on a periodic basis about eHealth's protection programs, with a focus on items such as current trends in the environment, incident preparedness, business continuity management, program governance, and program components, including updates on security processes, external testing, and employee training and awareness initiatives.

We are subject to various federal and state privacy and security laws, regulations and requirements. These laws govern our collection, use, disclosure, protection and maintenance of the individually identifiable information that we collect from consumers. We regularly assess our compliance with privacy and security requirements and will continue doing so as requirements evolve. eHealth is committed to implementing leading data protection standards.

Our Information Security Policy applies to all individuals that have access to eHealth information technology and data and workspace. It pertains to eHealth roles, supply chain partners, processes, and assets as applicable. The scope of the policy includes:

- All data created and/or maintained by eHealth, to include data of eHealth customers.
- All initiatives, projects, and activities that can impact eHealth's environment or the security of data, such as new systems development, replacements or enhancements to existing systems, ad hoc and prototype development, retirements, conversions, and outsourcing.
- Consumers who access eHealth systems to shop and buy insurance policies; these are referred to as "consumers" or "non-organizational users."
- Business partners (i.e., carriers) who access the eHealth system in order to access their data; these are referred to as "business partners" or "non- organizational users."
- Information systems, environments and platforms that are owned or leased by eHealth, that are used for eHealth business, including but not limited to, eHealth issued laptops and desktops, infrastructure, engineering and IT development environments, client/server environments, local, wide-area, and wireless networks, applications, software, tools, internet and intranet environments, email and tele-communication devices, on and off-site data storage, outsourced services that process eHealth information, and any other technology components; these are referred to as "information assets"

eHealth has acquired the following cybersecurity certifications: SOC2 Type 2, NY-DFS annual report, and PCI-DSS AOC. eHealth follows the SOC2 cybersecurity framework and completed the process of obtaining a HITRUST certification in the fall of 2024.

**Our HITRUST certification offers the following key benefits:**

**Risk management:** The certification process involved a rigorous risk assessment and the implementation of advanced security controls to mitigate potential threats to our systems. This proactive approach enhances our enterprise-wide risk management strategy, ensuring the resilience of our information infrastructure.

**Stakeholder confidence:** Earning HITRUST certification strengthens our credibility among clients, partners, and stakeholders. It demonstrates our commitment to data security, instilling confidence in those we serve and collaborate with.

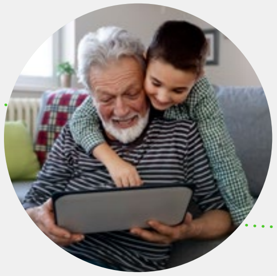
**Market leadership:** Achieving HITRUST certification positions eHealth ahead of many of its competitors, paving the way for future opportunities in business process outsourcing (BPO) and captive engagements.

eHealth's Privacy Policy can be found on our website by following this link. The policy contains details about how we collect, use, and share personal information that we obtain from interactions via our websites, email, mobile application, social media accounts, insurance agent and representative services, communication channels (including online chat and telephone call centers), in other online and offline interactions and services, and from other sources.

eHealth requires third party recipients to execute a written contract with eHealth containing appropriate confidentiality and/or privacy clauses that require reasonable care and adequate levels of protections, appropriate security measures, and allow data use only as described in the written agreement between eHealth and the third party. eHealth also performs reasonable due diligence checks prior to and during the selection of third parties who process consumer data on behalf of eHealth.

**Our comprehensive data security strategy includes:**

- Regular critical security assessments such as advanced attack simulations and vulnerability scans.
- A comprehensive Software Development Life Cycle (SDLC) framework to assess applications and related infrastructure before implementation to ensure our security standards are met.
- Use of a Role Based Access Control (RBAC) methodology, which defines the access a user receives to eHealth's information systems based on job function.
- Requirements that third-party vendors that host, transmit, or have access to eHealth data comply with our policies and undergo reviews.
- Monitoring of security event data and the security industry to flag anomalies and be aware of potential threats.
- Encryption of customer data both in transit and at rest.
- A broad spectrum of technical controls, including data loss prevention, role-based access, application/desktop logging, and data encryption, as well as multi-factor authentication and enhanced web application firewall controls.



We also conduct routine scans of our technical infrastructure and continuous penetration audits to check for vulnerabilities and meet our governance and compliance requirements. Training our employees and contractors is a crucial aspect of eHealth's governance and compliance requirements. All employees and contractors with access to an eHealth IT system complete security awareness training during onboarding and annually thereafter. Developers and privileged users are subject to additional security training requirements due to the increased inherent risk associated with these roles.

Every person with access to eHealth IT systems undergoes periodic phishing simulations and receives personalized tools to improve their security behavior. Performance is measured both individually and by functional groups to manage the maturity and improvement of eHealth's overall security posture. Employees must also acknowledge receipt and understanding of their responsibility to comply with eHealth's Code of Business Conduct, including the eHealth Information Security and Acceptable Use Policies, during onboarding and annually thereafter. eHealth additionally conducts annual Security Awareness Training and provides refresher training on targeted topics through a security-focused employee newsletter.

Information Security team is trained to contain any incident, mitigate impact, resolve or remediate issues, and notify affected parties as quickly as possible.

eHealth maintains an Incident Response Policy that outlines the procedures for handling a security incident. The policy provides the organization with a roadmap for implementing the structure for identifying, monitoring and resolving a security incident. The plan is distributed to all applicable members of eHealth leadership and the Incident Response Team. A cybersecurity overview is provided to both the CEO and the Board of Directors at least once per year.

Executives are subject to the same security training requirements as the rest of eHealth. In addition to these training requirements, eHealth's Senior Leadership Team participates in annual tabletop exercises that simulate a mock cyber-attack in order to build crisis management experience for our senior leadership and cybersecurity teams.