Health Information Exchange
Privacy & Security Controls

CORHIO collaborates with communities and stakeholders to implement secure systems and processes for sharing clinical information. Our policies to protect the privacy and security of personal health information are developed and maintained by a statewide policy committee consisting of diverse representatives from across the Colorado healthcare community. A cornerstone of this committee is our shared commitment to privacy and security for all participants and patients in the CORHIO HIE.

Our statewide, hosted HIE infrastructure, platform, and services are provided by the joint partnership between CORHIO and Health Catalyst (formerly Medicity).

Data Center	• HIPAA and HITECH compliant data centers (primary and backup) • SOC 2 Type 1 audited facility • CORHIO-specific cages • 24/7/365 hosted system monitoring and full failover capabilities • Offsite backup storage
Software & Services	• Comply with HIPAA and HITECH requirements for all services and deliverables • Annual Disaster Recovery/Business Continuity testing • Third party independent penetration testing • Up time, response time, RPO/RTO SLAs to support 24/7 operations for critical incidents • Intrusion detection • Anti-virus and risk assessment • Scheduled security updates
Data	Adhere to NIST guidelines for data encryption and backup media encryption
User Access	• Role-based access controls • Industry standard password strength and timeout requirements • User activities audited
Trained Workforce	• CORHIO workforce trained and accountable for upholding state and federal laws, including HIPAA, HITECH, and associated regulations, as well as all CORHIO policies and procedures • CORHIO Security Response Team consists of a Compliance Officer, a Privacy Officer and a Security Officer
Supporting Procedures	CORHIO maintains robust internal and external user policies including but not limited to: Appropriate Use of Services, Maintaining Authorized Users, Access Auditing, Inappropriate Use and Non-Compliance Reporting, System Security Safeguards, Filtering Sensitive Data, Breach Investigation and Notification
Patient Choice (Opt-Out)	Patients have the right to opt-out of participating in the HIE. Although clinical data will still flow among providers as it does today (e.g., lab results delivered to a provider from an independent lab), patients who do not wish to participate in the HIE will not have their data accessible in the community health record for query.

Colorado Regional Health Information Organization
4500 Cherry Creek S Dr. Suite 820
Denver, Colorado 80246

720.285.3200
www.CORHIO.org