CORHIO
HIE 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 consists of diverse representatives from across the Colorado health care community. A cornerstone of this committee is our shared commitment to privacy and security for all participants and patients in the CORHIO HIE.

Our hosted HIE infrastructure, platform and services are provided by a joint partnership between CORHIO and Medicity.

Data Center	• HIPAA and HITECH compliant data centers (primary & backup) • SAS 70 Type II 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 • Intrusion detection • Anti-virus and risk assessment • Scheduled security updates
Data	• Adhere to NIST guidelines for data encryption and backup media encryption • Confederated data model – all participant data separated on edge servers maintained inside the CORHIO data center
User Access	• Role-based authorized users • Industry standards password strength and session timeout requirements • User activities fully audited • Third party independent reporting and alerting on user patient access and user by org. access
Trained Workforce	• CORHIO and Medicity workforces trained and accountable for upholding laws and acts, HIPAA and HITECH compliance and any additional CORHIO HIE-specific policies • CORHIO Security Response Team consists of a Compliance Officer, a Privacy Officer and a Security Officer
Supporting Procedures	Internal and external policies and procedures such as: Appropriate Use of Services, Maintaining Authorized Users, Access Auditing, Inappropriate Use & 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.

4500 Cherry Creek S. Dr.
Suite 820
Denver, Colorado 80246

720.285.3200 TEL
720.285.3205 FAX

www.CORHIO.org