Health Information Exchange

Privacy and Security Controls

Contexture collaborates with communities and stakeholders to implement secure systems and processes for sharing clinical information. Contexture has developed policies to protect the privacy and security of personal health information. These policies are maintained by Contexture's Policy Advisory Council (PAC), which consists of diverse representatives and experts from the healthcare community in Colorado and Arizona. A cornerstone of the PAC is its commitment to privacy and security for all participants and patients in the Health Information Exchange (HIE).

Our statewide, hosted HIE infrastructure, platform, and services are provided through a partnership between Contexture and our vendors, Health Catalyst (formerly Medicity), and NextGen.

Data Center	■ HIPAA and HITECH compliant data centers (primary and backup) ■ SOC 2 Type 2 audited facility. ■ 24/7/365 hosted system monitoring and full failover capabilities. ■ Offsite backup storage.
Data	■ Adhere to NIST Guidelines for data encryption and backup media encryption.
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, Recovery Point Objective/Recovery Time Objective Service Level Agreements to support 24/7 operations for critical incidents. ■ Intrusion detection. ■ Anti-virus and risk assessment. ■ Scheduled security updates.
Patient Choice (Opt Out)	■ Contexture and our participants work together to ensure individuals have the information necessary to make a meaningful choice regarding whether their data is accessible through the HIE, as well as a process for implementing an individual's right to opt out of participating in the HIE.
User Access	■ Role-based access controls. ■ Industry standard password strength and timeout requirements. ■ User activities audited.
Supporting Procedures	■ Contexture maintains robust internal and external user policies including but not limited to: Permitted Use, HIE Notice and Opt Out, HIE Security and Maintenance, Incident Response, Security Safeguards, Access Control, etc.
Trained Workforce	■ Contexture's workforce is trained and accountable for upholding state and federal laws, including HIPAA, HITECH, and associated regulations, as well as Contexture policies and processes. ■ Contexture's Incident Response Team consists of the Chief Information Officer, Deputy Chief Information Officer, VP of Security, Chief Legal Officer, Director of Compliance.

Contexture relies on participants to establish and maintain internal policies and procedures that effectively manage access to, and the appropriate use of, Protected Health Information in the HIE System. If you have any questions regarding how Contexture safeguards HIE data, please contact the security team at **ccst@contexture.org**.