



Security and Compliance

Introduction

Clear Dx™ is a software-as-a-service (SaaS) offering for SARS-CoV-2 metadata analysis, placing high priority on protecting the confidentiality, integrity and availability of customer data. Clear Dx™ has a set of comprehensive policies, processes, and controls for security and privacy.

Clear Labs is implemented as a single instance, multi-tenant deployment. Bi-monthly updates are transparent, requiring no user action. All major upgrades are communicated via release notes at least 2 weeks in advance.

The software development life cycle of Clear Dx™ determines prioritization of features, content, functionality and bug remediation based on business needs and customer input. Software is engineered and unit tested using modern agile development methodologies. Service updates are scheduled with the customer to reduce the impact on operations. Changes are validated through automated regressions and manual testing, and it occurs in a test environment that is segregated from a staging/production environment.

To address platform security, Clear Dx™ combines Google Cloud Platform (GCP) encryption methods such as Encryption-at-Rest using AES-256 bit, Encryption-in-Transit using HTTPS over TLS 1.2, along with internal testing procedures. Together these methods provide a robust and secure cloud genomics solutions that exceeds the security provided by many institutional IT infrastructures.



We abide by HIPAA regulations strictly and have in place comprehensive compliance and security policies. Clear Dx™ utilizes Administrative, Physical, and Technical safeguards listed below to ensure the security and privacy of ePHI.

