LUMEDX Corporate Security Standards

The LUMEDX Corporation takes the privacy of patient and client data very seriously. We strive to exceed HIPAA, HITECH, ISO27001:2013 (with additional guidance from ISO27002:2013 and ISO 27799:2016), and data security/privacy standards in every possible area.

We purchase our SaaS hosting from internationally-recognized providers, deployed in regional datacenters protected by layers of defense-in-depth security. For non-SaaS clients, for details on our standards refer to the section “LUMEDX Corporate Security” later in this guide.

SaaS Security

1. Security standards
    a. ISO 27001 certified
    b. SSAE 16 certification
2. Physical security
    a. Video camera surveillance
    b. Monitoring by security personnel
    c. Secure entrances
3. Electronic security (data at rest)
    a. Forced client disconnect after 15 minutes of inactivity
    b. Data held on-shore (USA only)
    c. Active Directory authentication based on LDAP protocol
4. Communication security (data in transit)
    a. 256-bit minimum encryption of all transported data
5. Disaster recovery/backup and availability
    a. SQL database backed up continuously
    b. Apollo configuration data and tree backed up regularly offsite
    c. Software monitoring 24x7, including automatic alert and paging
6. Infrastructure
    a. Real-time communications networks, continuing through every area of the facility to each physical server unit
    b. Monthly patching
    c. Emergency change management process

LUMEDX Corporate Security

1. Security standards
    a. Compliant with ISO 27001, HIPAA, and HITECH, including annual audits
2. Physical security
    a. Secure building with keycard entry
    b. Help Desk area restricted to employees only
    c. Server room further restricted
3. Electronic security (data at rest)
    a. SQL databases encrypted
    b. 24x7 monitored firewall
    c. Intrusion detection
    d. Data Loss Prevention (DLP) on outbound email
4. Communication security (data in transit)
    a. 256-bit minimum encryption of all transported data
    b. Opportunistic TLS 1.1 for email
5. Disaster recovery/backup and availability
    a. Dual power supplies for all servers
    b. UPS for corporate server systems
    c. Temperature and moisture monitors in server room
    d. Backups (including activity logs) maintained for 7 years
    e. Software monitoring 24x7, including automatic alert
6. Employee training
    a. Workforce training includes an e-learning module that is updated annually and includes a test. Every workforce member retakes the test annually.