>ClearDATA

The ClearDATA Advantage

ClearDATA is the only healthcare exclusive cloud services provider to offer each customer a private cloud that is 100% compliant with HIPAA Security rules.

We are the healthcare cloud provider.

ClearDATA helps healthcare providers protect and manage their patient's electronic medical records, lower IT cost, and improve business agility. We understand healthcare business models, challenges, mandates, risks, industry language, and levels of IT sophistication and assistance required for: Practices, Hospitals, CAHs, IDNs, RECs, ACOs, Billing Cos, HIEs, Healthcare Hardware and Software Vendors, etc.

Cloud

We are experts in healthcare data and infrastructure management and information security with deep knowledge of how to design and deploy systems utilizing NIST standards in private cloud environments. We support EMR data and applications in an auditable, policy-driven HIT infrastructure. We help move healthcare IT infrastructure off-site into our state-of-the-art data centers, providing key customer benefits of: 100% uptime, fast application speed with high-performance bandwidth connections, offsite back-up and recovery and end-to-end security ensuring tightly managed HIPAA compliance policies and procedures.

Compliance

ClearDATA understands healthcare privacy frameworks, HIPAA privacy and security rules, and the patchwork of how more stringent regulations in states like California and Massachusetts impact data flows between hospital systems, physician practice groups, health information exchanges, patients, and the rest of the healthcare supply chain.

We assist in healthcare operations activities and therefore operate as a Business Associate. We provide Business Associates agreements as required to help protect our clients from unnecessary administrative liability,

Security

We are trained consultants that provide Security Risk Analyses in accordance with HIPAA Security Rule. The analysis assists in completing the measurements required to attest to Meaningful Use. We identify breach vulnerability and provide remediation plans for securing the Protected Health Information (PHI) of patients.

For network security, ClearDATA engineering establishes a Virtual Private Network between the provider and the data center. We use dedicated firewalls with enhanced security rules. Data is encrypted in motion and at rest at the disk level. We utilize strict policies, procedures and audit mechanisms through every component of the application and data storage solutions. We monitor and provide comprehensive reporting on user authentication, user access, what files or records were accessed and for how long.

EMR as a Service
HIPAA Cloud Hosting
Security Risk Assessment
Privacy & Security Consulting
Disaster Recovery

- **High Performance Private Cloud**
- **Offsite Data Backup, Recovery and Business Continuity**
- **Medical Image Storage**
- **Clinical Research Management**
- **Security Risk Assessments**
- **Privacy Impact Consulting**
- **Data Migration**
- **100% HIPAA compliance**
- **Business Associates Agreement**
- **End-to-End data encryption in motion and at rest at the disk level**
- **Strict Access Controls and Audit Mechanisms**
- **24/7/365 support including monitoring with alerts**

If you would like more information on ClearDATA products and services call 602-635-4006

HEALTHCARE · CLOUD · COMPLIANCE · SECURITY

Cloud Services

ClearDATA Private Cloud Services exclusively for Healthcare

ClearDATA Private Cloud Services fully automate and securely manage ePHI, applications, IT infrastructure and digital storage in our HIPAA compliant data center. Cloud configurations include operating system, CPU, memory allocation and disk storage including daily incremental and weekly full backups. Each network receives full service including configuration and enhanced monitoring services 24/7. Data is transported and stored in an encrypted state in motion and at rest in a full PHI compliant environment.

ClearDATA Offsite Backup, Disaster Recovery and Business Continuity

The ClearDATA Healthcare Data Backup and Disaster Recovery Service provide HIPAA-compliant, off-site storage of data and applications. The data is encrypted in motion and at rest and is stored in a secure storage network with backup accessibility to the file level. Our Disaster Recovery Service includes a managed disaster recovery plan to match the business needs of your applications and data to your recovery objectives ensuring you are back in operation according to your recovery strategy.

Our service enables healthcare providers to securely store their data offsite to meet compliance requirements. The data is accessible to the file level and fully encrypted. To prevent minimal downtime in a disaster, we provide a managed disaster recovery service that brings their applications and data back in operation according to the application and data business requirement for business continuity.

ClearDATA Medical Image Storage and Archiving

We lower the cost of medical image storage. Digital technology advancements are improving the ease, capture and use of medical imaging.   Medical images can consume large amounts of storage, requiring the business to continually invest in additional storage hardware. ClearDATA Medical Image Archiving provides economical HIPAA-compliant off-site storage of medical images in a vendor neutral, DICOM-compliant cloud storage network. Cloud based image storage provides expandable storage on an as needed basis, charging only for what's used. The business no longer needs to "buy ahead" in anticipation of data not yet created.

ClearDATA Clinical Research Management Cloud Platform

The ClearDATA Clinical Research Management Cloud Platform helps make research studies available to a greater number of research facilities and partners. We lower the cost of studies by providing leading Clinical Research Management software in a highly-scalable cloud platform while charging only for the resources you use – applications, computing and storage. By reducing the costs of a clinical research project, ClearDATA enables a greater number of the research facilities to access studies that were previously unavailable due to insufficient technological and financial resources. This solution is available for enterprise, departmental and small study group organizations and is being used in the leading clinical research institutions.

ClearDATA Data Migration and Virtualization

ClearDATA provides our clients with data migration services. We assist them in capturing and safely migrating their existing on-premise data and systems into the ClearDATA infrastructure. Once the migration strategy is defined, ClearDATA provides complete migration and cutover services to eliminate downtime and any single points of failure. The strategies include secure mirroring, incremental backups of the mirror, disk-level encryption, secure VPN, and managed Secure Socket Layer (SSL) services.

Security and Privacy Services

HITECH Meaningful Use Criteria HIPAA-Compliance Security Risk Assessment

The USHC Security Risk Assessment (SRA) is focused specifically on 45 CFR 164.308(a)(1); with in-depth analysis of the four safeguard areas, the Administrative, Physical, Organizational and Technical safeguards. Each of these areas is analyzed to verify that they are: a) sufficient to be effective, b) currently operational, c) applicable for the organization and d) represent applicable compliance programs. Additionally, we review the organization's vendor relationships and Business Associate Agreements, and if necessary, conduct an SRA for the Business Associate. The deliverable is a final assessment identifying all threat risk / vulnerabilities and an executive briefing report appropriate for an executive and/or Board meeting, along with a complete risk remediation roadmap.

Prepare Policies & Procedures Documentation

Some companies prefer that USHC create and manage the P&P manual based on the assessment to save time and money. USHC will create a customized P&P manual and tailor it specifically for the organization, workflow and personnel. Outsourcing the documentation development and preparation, especially when combined with the Security Risk Assessment, ensures a complete "go to" manual that can be used by anyone in the practice to find procedures and forms to manage all aspects of HIPAA compliance.

Polices & Procedures Update Subscription

As new EHR modules are added, as regulations are revised, or as employees come and go, the P&P manual needs to be updated accordingly to stay consistent with regulatory and business changes. We will review and update policies and procedures quarterly to incorporate the latest changes and provide a briefing to your security official and if requested engage training personnel on these changes.

Online HIPAA Training Module

Training is essential to maintaining the adherence of policies and procedures to minimize risk and the devastating impact of a breach. Our Online Training Module provides the HIPAA workforce with an understanding of the policies and procedures and tests for knowledge. This is a great tool for new employees to get up to speed regarding HIPAA P&P.

Remediation Assistance

Once the SRA is completed, we can help the remediate any issues from the assessment. The assistance can range from choosing a software vendor, advising on technology, to simple day-to-day solutions to minimizing vulnerability.

Security & Privacy Compliance Official

In order to meet HIPAA administrative compliance, the entity is required to designate a Security and Privacy Official who is responsible for maintaining compliance with the HIPAA Privacy and Security Rules. USHC can provide a Chief Privacy Officer or Chief Security Officer on retainer who can work directly with an administrative manager on a monthly basis to ensure the business is managing its policies, procedures, and privacy programs effectively.

Privacy Impact Assessment

The USHC Privacy Impact Assessment (PIA) is an assessment of the privacy impact of any substantially revised or new Information Technology System. A PIA guides a healthcare provider's project team through a series of stages in order to identify the privacy risks and suggests methods of mitigating or eliminating them. The focus of a PIA is on the patient information and the impact of a new system introduced to an existing environment and its effect on your current privacy policies and procedures.