

HIPAA Statement

Dicom Systems Unifier Enterprise Imaging Platform

Version 2.5.1 | (August 30, 2019)

Dicom Systems, Inc.

HIPAA Compliance Statement

The US Congress passed the Health Insurance Portability and Accountability Act (HIPAA) in 1996, which became effective starting from 1997. The Administrative Simplification provision of HIPAA was developed to reduce the costs and administrative burdens of health care by making it possible to replace manual transactions on paper with standardized electronic transactions. The Administrative Simplification provisions of HIPAA also address the security and privacy of health data. Dicom Systems has implemented the provisions into our software solutions to provide means for health care providers to comply with the HIPAA regulations.

Dicom Systems, Inc. is committed to and has implemented many safeguards to ensure its devices, services, websites and data systems (collectively “Products”) are compliant with the regulations and conditions set forth in the Health Insurance Portability and Availability Act of 1996 (HIPAA). Dicom Systems is committed to continuous improvement to ensure Dicom Systems Products incorporate state-of-the-art information technology privacy and security measures.

As a Business Associate per the definition in the HIPAA Act, and by assignment of the HIPAA covered entity, Dicom Systems is subject to the following controls:

Administrative Safeguards (HIPAA 164.308). Dicom Systems has implemented policies to ensure appropriate assignment of data access permissions and proper movement and handling of Protected Healthcare Information (PHI). HIPAA training is an annual mandated event for all Dicom Systems employees, as well as annual review of policy effectiveness during internal auditing of our Products and Quality System. Certificates of HIPAA training for all employees are kept on file and are available upon request.

Physical Safeguards (HIPAA 164.310). Dicom Systems’ primary physical safeguard is to not retain sensitive data in any public or private Dicom Systems location other than those assigned for internal database management, quality assurance activities and technical support. Access to Dicom Systems corporate offices are all independently controlled via card access preventing walk-up intrusion. Dicom Systems does not own or operate its own data center; Dicom Systems uses third-party infrastructure providers that operate cloud-based architecture with inherent security measures including 24 hours monitoring, advanced fire protection systems, uninterruptible power and database redundancy. Annual audit of the facility security plan, disaster recovery plan, and contingency plans are in place. All Dicom Systems customers deploy Dicom Systems appliances within their own infrastructure, or within a third-party operated IT infrastructure that they have independently audited for HIPAA compliance, and

whose services they have contracted independently of Dicom Systems (Google Cloud Platform, Amazon Web Services, Microsoft Azure, among others).

Technical Safeguards (HIPAA 164.312). To further protect sensitive data, Dicom Systems enforces unique software architecture that includes user identification and authentication, various database audit logging, data integrity systems and verified backups, entity authentication programs, digital certificates, various levels of encryption, certificates and other custom architecture to further obscure sensitive data from threats, and to mitigate potential vulnerabilities.

This provision of the law required the Department of Health and Human Services (DHHS) to develop standards (also called rules or regulations) for the maintenance and transmission of Protected Healthcare Information (PHI). These standards were developed to:

- Improve the efficiency and effectiveness of the health care system by standardizing the interchange of electronic data for the specified transactions
- Protect the security and confidentiality of electronic health information. Dicom Systems enables our customers to implement HIPAA-compliant security features due to our proactive product development. Specifically, Dicom Systems Unifier allows our customers to enable the following features, policies and restrictions:
 - The ability to implement, administer and enforce strong password policies
 - The ability to ensure integrity, authenticity and confidentiality of communication between Dicom Systems Unifier components
 - The ability to audit user activity
 - The ability to export detailed logs to external applications
 - The ability to require that systems utilize certificates in order to transmit protected healthcare information (PHI)
 - The ability to restrict user access to a specific selection of medical information
 - The ability to prevent unauthorized access to images in the Dicom Systems appliance's local cache by means of encryption
 - The ability to anonymize images that are displayed or exported by the Dicom Systems Unifier platform
 - The ability to ensure high availability of images at all times by architecting and maintaining solutions that keep multiple copies of all images, and high availability of the systems that make the images available to end-users

Privacy and security are essential components of our software solutions. Dicom Systems Unifier software enables functionality, which when properly configured and implemented, allows Dicom Systems Unifier customers to be fully compliant with all pertinent aspects of HIPAA. Dicom Systems Unifier endorses the security standards raised by HIPAA and we are committed to enabling our customers to protect patient privacy.

For more information about how Dicom Systems handles HIPAA-related matters, please email regulatory@dcmsys.com.



Label

Product: Unifier Enterprise Imaging Platform
Version: 3.5.20-1



LT-CA01/MDD/1-00015/15

Official Correspondence

Dicom Systems Inc
1999 S. Bascom Ave. Ste 700
Campbell, CA 95008 United States
(415) 684-8790
dcmsys.com

FDA Listing Detail

| | |
|--------------------------|----------------|
| Device Type: | Class I Device |
| Registration/FEI Number: | 3009132733 |
| Listing Number: | D120970 |
| Listing Status: | Active |
| Submission Type: | 510(k) exempt |