

***HIPAA Compliance Statement***

***Objective Data Storage LLC. (ODS Medical)***

***Monday, June 12, 2006***

***Version 1.00***

Objective Data Storage LLC.  
Copyright © by Objective Data Storage LLC 2006

All Rights Reserved. Printed in the U. S. A.

## Compliance Statement

Compliance with state and federal regulations regarding patient confidentiality, security, and privacy is the responsibility of all health care providers and related vendors. This includes, but is not limited to, compliance with the Health Information Portability and Accountability Act (HIPAA) of 1996. The Health Insurance Portability & Accountability Act was written into law on August 21, 1996. HIPAA regulations will have an effect on operational procedures on all healthcare provider organizations.

HIPAA recognizes that the largest task in compliance is administrative, not with the technical features of computer systems. That administrative task primarily involves policy and procedures, establishing a system security and information confidentiality policy, training all personnel in that policy and appointing a “security officer” to monitor compliance with the policy.

HIPAA regulations stress “reasonable and appropriate” security measures that address the particular institution’s security needs, risks, and business requirement. On the technical side, each institution will need to assess systems, systems vulnerabilities, and evaluation of compliance to both HIPAA and to the institution’s security policy. This is a significant challenge as it involves consideration of the operational procedure of healthcare provider organizations.

There is no way to assert HIPAA compliance for software or hardware products. It is the organization that is compliant, not the products they use but how they are used. Since an organization’s needs, policies and procedures may be quite different, the solutions will be policy related. Technology should play a role of enabling organizations to put into effect policy. Rather than discussing HIPAA compliance for products, ODS Medical’s strategy is to share information on the security and privacy features of our products, and how those features can help healthcare organizations security procedures.

**ODS Medical** is aware that complying with HIPAA is important to system healthcare organizations as they move to meet distribution, transaction security and privacy regulations by 2003.

**ODS Medical** works closely with OEMs and VARs regarding healthcare customers questions and concerns related to planning and maintenance of PACS implementation so that confidentiality and security is promoted. Our medical storage and exchange products are constantly being updated to include mechanisms that assist system administrators to implement privacy and security policies. We are committed in working with end-users to provide additional value to help healthcare facilities meet the continuing HIPAA challenge.

**ODS Medical** has been providing configurable storage and distribution systems that protect the privacy and security of organizations and patient’s confidentiality. Our software and products already incorporate many of the core HIPAA requirements.

**ODS Medical** offers a set of DICOM 3.0 compliant storage products that also comply with HIPAA and other privacy and security requirements. ODS Medical provides not only technical and

workflow recommendations for products but also features quality assurance features that allow end users HIPAA compliance programs.

User name and log-on are required for all users accessing **ODS Medical** systems via GUIs. Most access to data is performed via the DICOM 3.0 protocol. **ODS Medical's** products completely adhere to the DICOM 3.0 standard. **ODS Medical** strongly discourage any user from sharing or disclosing his or her password or user name.

**ODS Medical's** medical software provides an audit trail of all electronic events related to any patient's medical record within the system. The log can be viewed or copied to an external databases (e.g., Access) or spreadsheets (e.g., Excel) for further analysis.

**ODS Medical** encourages all customers to have backup copies of all their medical imaging records. The ODS PACScomm product line includes optional features to enable making backup copies.

**ODS Medical** supplies fault tolerant storage servers and other related technologies to support disaster planning.

**ODS Medical** promotes placing computer technology in appropriately secured and confidential areas with enough ventilation and electrical power in order to reduce unauthorized access to systems and volumes containing patient data.

**ODS Medical's** software requires user names and passwords to generate, edit, revise, or correct data. Systems keep logs when different events occur. ODS Medical offers a set of mechanisms that allow system administrators to implement different levels of security on different system components based on their use and location. Appropriate confidentiality notices are displayed on screens when records are queried using **ODS Medical's** GUIs whether it is done locally or over the network.