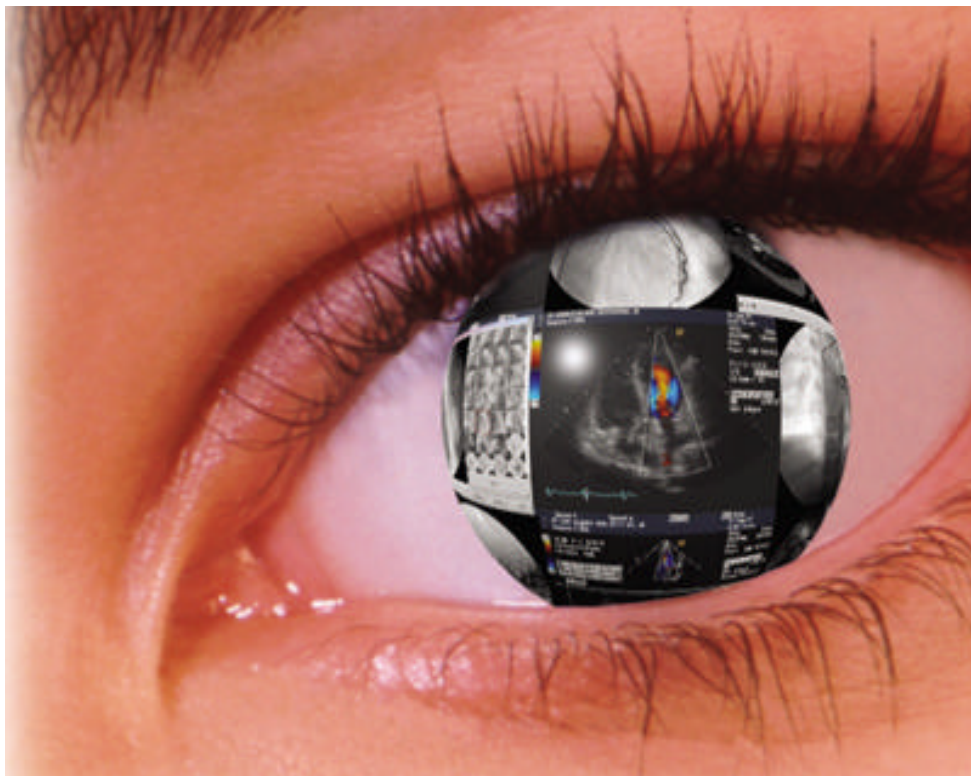




The Image Management and Archival System

HIPAA Compliance Statement



Since some HIPAA regulations have not been concluded yet this document will be modified as the standard becomes available.

**OptiMed Technologies, Inc.
20 New Dutch Lane, Fairfield, NJ 07004 USA
Telephone: (973) 575-9911 * Fax: (973) 575-9722 * Customer Service: (800) 411-9999**

©2004, OptiMed Technologies, Inc.

All rights reserved. Printed in USA.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form, by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of OptiMed Technologies, Inc.

Table of Contents

1	Introduction	4
2	Personal Security and Administration	4
3	Security Management	4
4	Data Integrity	4
5	Database	4
6	Access Control	5
6.1	Operating System Level.....	5
6.2	Application Level.....	5
6.3	Unique Identifiers (biometric devices).....	5
7	Change of Password	5
8	Encryption	5
9	Remote Access	5
9.1	RAS.....	6
9.2	Callback.....	6
10	Auto Logoff	6
11	Audit Trail	6
11.1	Operating System Event Files.....	6
11.2	Application Log Files.....	6
11.3	Database Log Files.....	6
11.4	Storage Log Files.....	6
11.5	Internet Audit Trail.....	6
12	Data Backup	6
13	Disaster Recovery	7

1 Introduction

The purpose of this document is to detail OptiMed's compliance with the various features of the HIPAA regulations. In order for a healthcare provider to be compliant with HIPAA regulations, policies and procedures need to be in place to work along with the security measures addressed on a technical level. OptiMed's products provide compliance on a technical level, guarding data integrity, confidentiality and availability. Each individual healthcare provider is responsible to ensure compliance on a physical and administrative level, establishing policies in order to maintain the privacy and security of patient information.

At times OptiMed will be made aware of certain protected health information and is, therefore, considered a "Business Associate" of its' customers. In line with the HIPAA regulations, OptiMed is required to sign a Business Associate Agreement for its' customers.

2 Personal Security and Administration

It is the hospital's responsibility to create accounts, user rights and access control for its users. It is also the hospital's responsibility to provide the physical location of the equipment as well as the proper security measurements required by the HIPAA regulation.

3 Security Management

OptiMed will provide the material necessary to analyze its compliance with the HIPAA regulations. It is the hospital's responsibility to provide a name of the designated manager for the HIPAA security.

4 Data Integrity

OptiMed's system contains built-in mechanisms to test and ensure data integrity. The system is using a standard data format (i.e., DICOM), checksum mechanism and WORM technology for securing and assuring data integrity.

5 Database

HIPAA regulations require adding unique fields to each record in the database. These fields are included in OptiMed's database.

6 Access Control

OptiMed provides different levels of access control.

6.1 Operating System Level

The application is currently running on M.S. Windows 2000, M.S. Windows XP and M.S. Windows 2003 operating systems, which are DOD C2-level compliant. These Operating Systems provide tools for access control, including user authentication, authorization and audit. Administrator may achieve high level of access control granularity.

6.2 Application Level

OptiMed provides a utility to allow the administrator to create groups of accounts by which one group cannot access records of another group. Each login user is compared against the physician name on the patient record. If the login user and the name on the record are from the same group, the record can be accessed. For specific user needs application may set access rights per image.

6.3 Unique Identifiers (biometric devices)

OptiMed's system supports biometric devices (fingerprint, retinal scan, etc.) for unique identification. All biometric devices are combined with user login and password.

7 Change of Password

The Operating systems used by the OptiMed system (2000/XP/2003) support the enforcement of change of password. It is the administrator's responsibility to define the frequency of password change.

8 Encryption

OptiMed supports HIPAA Encryption rulings both by software and hardware.

9 Remote Access

OptiMed is using a remote access tool for service purposes. The remote tool supports different security mechanisms.

9.1 RAS

This mechanism provides a remote access via user account using login and password.

9.2 Callback

This mechanism provides a callback to verify the caller identification.

10 Auto Logoff

OptiMed's application provides an auto logoff mechanism with a time variable that can be preset. This mechanism exits from the account to the login screen if the system was not used within the preset time.

11 Audit Trail

The system provides a few different audit trails:

11.1 Operating System Event Files

Operating System event files are tracking system errors and events.

11.2 Application Log Files

Application log files are tracking application errors, events and activities.

11.3 Database Log Files

Database log files track database activities and manual modifications.

11.4 Storage Log Files

Storage log files are tracking activities on the long-term storage device.

11.5 Internet Audit Trail

Internet audit trail is tracking activity and access of system via Internet and Intranet.

12 Data Backup

OptiMed can provide the hospital with the tools (hardware and software) necessary to backup its data at a remote location. OptiMed also provides the capability for the hospital to provide its own tools for data backup. In any case, it is the hospital's responsibility to designate a person(s) to manage the backup task.

13 Disaster Recovery

OptiMed's data backup solutions provide a means for the hospital to have information available for storage at a remote location in case of disaster. It is the hospital's responsibility to provide a contingency or disaster recovery plan for such situations that will ensure the availability of information.