



Fulfillment of HIPAA Requirements

White Paper

November 20, 2003

ABOUT ALTIRIS

Altiris, Inc. is a pioneer of IT lifecycle management software that allows IT organizations to easily manage desktops, notebooks, thin clients, handhelds, industry-standard servers, and heterogeneous software including Windows, Linux, and UNIX. Altiris automates and simplifies IT projects throughout the life of an asset to reduce the cost and complexity of management. Altiris client and mobile, server, and asset management solutions natively integrate via a common Web-based console and repository. For more information, visit www.altiris.com.

NOTICE

The content in this document represents the current view of Altiris as of the date of publication. Because Altiris responds continually to changing market conditions, this document should not be interpreted as a commitment on the part of Altiris. Altiris cannot guarantee the accuracy of any information presented after the date of publication.

Copyright © 2004, Altiris, Inc. All rights reserved.

Altiris, Inc.
588 West 400 South
Lindon, UT 84042

Phone: (801) 226-8500
Fax: (801) 226-8506

BootWorks U.S. Patent No. 5,764,593.
RapiDeploy U.S. Patent No. 6,144,992.

Altiris, BootWorks, Inventory Solution, PC Transplant, RapiDeploy, and RapidInstall are registered trademarks of Altiris, Inc. in the United States.

Carbon Copy is a registered trademark licensed to Altiris, Inc. in the United States and a registered trademark of Altiris, Inc. in other countries.

Microsoft, Windows, and the Windows logo are trademarks, or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Other brands and names are the property of their respective owners.

Information in this document is subject to change without notice. For the latest documentation, visit www.altiris.com.

CONTENTS

Introduction..... 1
Management of Customer-Facing Records..... 2
 Associating Contact Records to Relevant Assets and Resources 2
 Support through Role-and-Scope-Based Security 2
More Information..... 7



INTRODUCTION

HIPAA includes provisions designed to encourage electronic transactions and also requires safeguards to protect the security and confidentiality of health information.

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is designed to protect patients' medical records and other health information provided to health plans, doctors, hospitals, and other health care providers. HIPAA includes provisions designed to encourage electronic transactions and also requires safeguards to protect the security and confidentiality of health information. The regulation covers health plans, health care clearinghouses, and those health care providers who conduct certain financial and administrative transactions (for example, enrollment, billing, and eligibility verification) electronically.

MANAGEMENT OF CUSTOMER-FACING RECORDS

Many software applications manage contact records containing patient or employee healthcare information. This information can be stored in databases, servers, workstations and contact records themselves. Customer Relationship Management (CRM) solutions and Human Resources applications are the most commonly affected by the management and security of patient and employee records. These applications are typically considered "customer facing" and are used by call centers to gain detailed information about the patient/employee, including health records to better service the patient/employee.

Associating Contact Records to Relevant Assets and Resources

Altiris Solutions capture information about IT assets and infrastructure (may include hardware, software, peripherals, furniture) and associates contact records to relevant assets and resources. The purpose of such records is dedicated to IT infrastructure as opposed to patient or employee health records. Altiris users access contact data to better understand the relationship of users to assets, locations, departments, cost centers and contracts where health records are not pertinent. In the unlikely event that Altiris solutions are used to store health-related data, Altiris can secure the data through utilization of role and scope-based security. Role and scope-based security is designed to create roles within the system to define security parameters for user privileges, only allowing authorized users to access relevant data or reports.

Support through Role-and-Scope-Based Security

Altiris solutions support HIPAA requirements through role and scope-based security to block access to unqualified users, utilization of a unique security ID, public and private data encryption, audit controls, integration with Active Directory, back-up and recovery of mission critical environments, and removal of pertinent data from machines during reallocation, retirement or disposal.

Altiris' strengths in IT lifecycle management, application usage, patch management, backup and recovery, and overall systems management support addresses the HIPAA requirements of:

- Intrusion detection
- Impact assessment and recovery
- Vulnerability assessment
- Policy compliance
- Software verification

Overall, Altiris also addresses HIPAA requirements in these areas:

| | Description |
|-----------------------------------|--|
| Contingency Plans | <ul style="list-style-type: none"> Applications and data-critical analysis Data backup planning Disaster recovery and business continuity planning Emergency mode operation planning Client and Server provisioning, testing, and re-visioning procedures |
| Information Access Control | <ul style="list-style-type: none"> Access authorization Access establishment Access modification |
| Internal Audit | <ul style="list-style-type: none"> In house review of system records of system activity (including logins, file accesses, problem fix and incident tracking) |
| Security Configuration | <ul style="list-style-type: none"> Hardware and software installation, maintenance reviews Build testing Software package and build testing Virus checking and remediation |
| IT staff and End User | <ul style="list-style-type: none"> Training and professional services are available to ensure enterprises gain access to best practices principles, procedures, and functionalities |

Note: Additional explanations are specified below.

| Section | Standard | Specification | Capability |
|------------------|----------------|---------------------------|--|
| Technical | | | |
| 164.312(a)(1) | Access Control | Unique User ID | Console is browser enabled with unique log-on ID and passwords. Advanced systems administrative controls are embedded using the latest Microsoft standards and Altiris architecture. |
| | | Emergency Access | Organizations must establish policies and procedures to help ensure access to necessary electronic protected health information during an emergency. |
| | | Automatic Logoff | Application sessions are protected by the ability to set automatic signoff for specified durations. |
| | | Encryption and Decryption | Altiris allows organizations to encrypt and decrypt information with public and private keys as it is sent over a public or private network. |
| | Audit Controls | | With Altiris, organizations can determine who launched what applications from which locations at particular times. Event messages generated by system activities across an organization's various operating systems and applications can be collected, normalized and stored in the central repository. Database-driven querying, filtering and reporting can be performed on demand. The ease and efficiency helps reduce effort and Auditing expenses. Centralized alerting can be automatically triggered upon detecting patterns of events. Potential damages are constrained and business-critical resources can be adjusted based on risk mitigation and damage minimization policies. |

| Section | Standard | Specification | Capability |
|-----------------|---------------------------|--|---|
| Physical | | | |
| 164.310(a)(1) | Facility Access Controls | Contingency Operations | The disaster recovery plan and/or emergency mode operations prescribes facility access policies to support restoration of lost data. |
| | | Facility Security Plan | Organizations should enact policies and procedures that safeguard facility and equipment against unauthorized physical access, tampering or theft. |
| | | Access Control and Validation Procedures | Protect access to critical workstations and servers by effective physical access control methods. This is further supplemented by role-and-scope-based access privilege controls that Altiris applies to system administrators and end users. |
| | | Maintenance Records | HIPAA covered entities must develop policies and procedures that enable documenting repairs, modifications. Altiris' leading approach to lifecycle management enables cradle-to-grave tracking of vital IT and related assets. |
| 164.310(b)(1) | Workstation Use | | Based on their role, users are able to access and use only those functions for which they are authorized |
| 164.310(c) | Workstation Security | | Organizations must implement physical security measures to restrict workstation access to authorized users only |
| | Device and Media Controls | Disposal | Policies and procedures control receipt and removal of hardware and electronic media that contain electronic protected health information into and out of the facilities. |
| | | Media Reuse | Organizations must establish policies and procedures to eliminate public health information from all media, before that media may be cascaded, re-cycled or de-commissioned. |
| | | Accountability | The Altiris suite of IT lifecycle management products (including Asset Control Solution) can be used to log the assignments and the use of IT resources that may contain public health information. Additionally, the location, movement, depreciation, and contracts related to responsibilities for such information can be recorded, managed and archived. |

| Section | Standard | Specification | Capability |
|-----------------------|----------------------------------|-------------------------------------|--|
| Administrative | | | |
| 164.308(a)(1) | Security Management Process | Risk Analysis | Security risks appear in many ways from internal and external sources. Altiris systems management capabilities and reports allow organizations to monitor network activity and help reduce intrusions. For example, application metering, patch management and recovery work together to monitor usage, rectify vulnerabilities, and roll back to prior steady state. |
| | | Risk Management | Risk management is required to reduce the quantity and level of potential security vulnerabilities. Altiris products enable establishing policies, collections, and notifications that can significantly improve risk management for HIPAA-covered entities. |
| | | Sanction Policies | Organizations must develop internal policies and procedures to apply appropriate sanctions to workforce members and contractors who are provided access to information, reports and equipment but may violate or fail to comply with established security policies and procedures. |
| | | Information Systems Activity Review | Altiris allows organizations to monitor performance and track system activity, access attempts, unauthorized applications, and malicious software from a user and network perspective. The configuration management database also contributes to the monitoring process by consolidating appropriate status, activity, and change information. |
| 164.308(a)(2) | Assigned Security Responsibility | | Organizations must identify the security officer who is responsible for the development and implementation of the policies and procedures required by HIPAA regulations. |
| 164.308(a)(3) | Workforce Security | Authorization and/or Supervision | To properly authorize workforce members, organizations should set up role-based authorization policies to establish an appropriate level of access privileges. Altiris integrates natively with Active Directory to centralize, record and manage user assignments and activities. Establishing relationships of the users' who, what, where and why helps ensure that assets, data, reports, analysis and business intelligence are available to the organization attaining HIPAA compliance and overall systems manageability success. |

MORE INFORMATION

For more information, visit www.altiris.com.