

Achieving HIPAA Compliance With Identity Management from Sun

A Business White Paper
September 2004



Table of Contents

HIPAA: A Top Executive Concern	1
HIPAA Compliance in Large Organizations	2
End-to-End Identity Management From Sun	4
Role-Based Access Controls	4
Effective Account Management	5
Reasonable Safeguards	6
Termination Procedures	6
Entity Authentication	7
Password Strength Enforcement	7
Implementation of Identity Management Systems	8
Sun Identity Management: A Key Component for HIPAA Compliance	11
About Sun	11

Chapter 1

HIPAA: A Top Executive Concern

Healthcare Insurance Portability and Accountability Act (HIPAA) regulations and consumer demand for protection of healthcare information have made the controlling of access to information systems a top concern among IT professionals and corporate executives. Implementing effective and efficient controls to protect the privacy and security of protected health information (PHI) involves the coordination and effective use of available technology and products.

In a recent survey of over 800 healthcare information executives, 56 percent of respondents said they plan to upgrade their systems to become compliant with HIPAA as part of an HIPAA compliance effort. And because of the high reliance on information systems to protect PHI, nearly 100 percent of all HIPAA compliance teams within organizations include members from the information technology department.

It should be no surprise that HIPAA is such a high concern. Nearly every customer, business partner, regulator, and lawyer is looking to the organization's top executives for answers to their HIPAA compliance progress. Looming deadlines, fines of up to \$100,000, and prison terms of up to five years for noncompliance elevate the importance of HIPAA compliance as well.

Many organizations are finding that the HIPAA regulations "run deep" and affect many elements of the business process, information systems operation, and information systems management. In-house solutions that consist of developing policies and procedures from scratch and implementing custom applications and modifications to the existing information systems are time-consuming and typically ineffective. What is needed is a proven solution with HIPAA-compliant features. Using HIPAA-compliant privacy and security features in available technology — such as that found in Sun's identity management solutions — is an efficient and effective way of implementing a HIPAA compliance program within large healthcare organizations.

Chapter 2

HIPAA Compliance in Large Organizations

At its core, HIPAA is about taking steps to protect the confidentiality of patient information. Achieving HIPAA compliance means implementing security standards that govern how healthcare plans, providers, and clearinghouses transmit, access, and store protected health information in electronic form.

HIPAA privacy regulations require that the use of personal health information (PHI) be limited to that which is minimally necessary to administer treatment. Such limitations must consider the effects of various provisions for parents and minors, use in marketing, research, payment, and government access on authorization decisions.

HIPAA security regulations further impose requirements to develop and enforce “formal security policies and procedures for granting different levels of access to PHI.” This includes authorization to access PHI, the establishment of account access privileges, and modifications to account privileges. Furthermore, the HIPAA security regulations require the deployment of mechanisms for obtaining consent to use and disclose PHI.

Due to the number of users, the complexity of data classification, the dynamic nature of organizations, and the interconnection of information systems, it can be extremely difficult for organizations to support HIPAA privacy and security regulations.

- **Multiple Information Systems.** The scope of control for PHI is expanded greatly by the sharing of PHI within various information systems within the organization as well as the sharing of PHI with associates outside of the organization. Large healthcare organizations share information across a multitude of systems, from payroll and patient processing to employee databases and business associate networks. Keeping track of user accounts and patient information, and enforcing appropriate access control policies, can be difficult in such far-reaching and heterogeneous environments.
- **Complex Roles, Data Classification, and Authorization.** To effectively enforce HIPAA privacy rules for consent and limit the use of PHI to the minimum necessary, large healthcare organizations must establish and maintain a complex structure of PHI access classes for the data, roles, and privileges for users as well as authorization decisions for users’ interaction with PHI data.
- **Large and Growing Number of Accounts.** Information systems within large organizations support thousands, even tens of thousands, of users in a variety of roles. The sheer number of accounts, users, roles, and authorization decisions requires effective processes and controls to ensure adequate protection of PHI.

- **Dynamic and Volatile Nature of Accounts.** Frequent changes in who is allowed access to what information multiply the already complex task of access control. Events such as employee turnover, emergency access, promotions, job rotations, and changes in agreements with business associates all require the associated changes in the access control mechanisms. Many of the personnel assigned to these roles change frequently, while other accounts are temporary or require increased level of access for a short amount of time. This dynamic nature of accounts, privileges, and access levels makes the task of account provisioning, maintenance, and termination one of the most difficult tasks in the secure operation of these information systems.
- **Availability of PHI.** The unavailability or temporary loss of medical records containing PHI can impair delivery of healthcare services and business operations. While some unavailability may be caused by weather or external physical forces, organizations should reduce opportunities for downtime from IT upgrades and backups and ensure unplanned outages are minimized. Organizations must develop downtime procedures that can be used while networks are restored or backups are reloaded. In addition, enterprises should design and deploy infrastructures that provide backup operations to minimize downtime and protect PHI during outages.
- **Evolution of the Virtual Enterprise.** Enabling the virtual enterprise requires a network platform comprised of common protocols, interfaces for communicating, and the ability to share data and conduct transactions across all platforms. Healthcare providers, insurance companies, pharmaceutical companies, and others are working more collaboratively because of the need to manage access and exchange of data securely and according to policy. This need has heightened the awareness of federation, and has brought to the forefront the need for interoperability and integration standards.

Chapter 3

End-to-End Identity Management From Sun

Sun's comprehensive identity management product line facilitates the enforcement of HIPAA privacy and security regulations through the efficient management of identity data, entitlements, and permissions. Sun provides everything an enterprise needs to securely manage user access to sensitive information, including:

- **Sun Java™ System Identity Manager** is a noninvasive and secure user provisioning and data synchronization solution that uses automation and delegation to reduce the time and costs associated with enabling new users to start working productively and instantly disabling access when relationships change or end for a more secure enterprise. Java System Identity Manager also provides a complete password management solution that enables end users to manage their passwords themselves, increasing their satisfaction while greatly reducing associated support costs.
- **Sun Java System Access Manager** provides decentralized authentication and authorization services across internal and external computing domains and ensures that appropriate authentication credentials are required of users depending on the value of the protected resources. Java System Access Manager makes certain that authorized users have access to specific resources while simultaneously protecting those resources from unauthorized users. It presents streamlined navigation across enterprise Web applications through single sign-on capabilities, and also enables the enterprise to audit all access activities, including authentication attempts, authorizations, and changes made, to assist in complying with regulatory audit requirements.
- **Sun Java System Directory Server Enterprise Edition** delivers secure, highly available, and scalable directory services for storing and managing accurate and reliable identity data. It serves as the backbone to an enterprise identity infrastructure, enabling today's mission-critical enterprise applications and large-scale extranet applications to access consistent, accurate, and reliable identity data for significant operational and cost efficiencies. Java System Directory Server Enterprise Edition integrates smoothly into multiplatform environments, and provides secure, on-demand password synchronization with Microsoft Windows Active Directory.

Role-Based Access Controls

Identity Manager filters access control requests based on role- and rule-based access controls. These access control models allow complex access control decisions to be modeled and implemented in automated systems. Role-based access control (RBAC) allows access control decisions to be based on the role currently being performed by an individual. Access Manager ensures that security policies can be centrally enforced, resulting in improved security and simplified management by utilizing a central point of authentication and role- and rule-based access control.

For example, a physician taking a shift in the emergency room would access the system using his temporary role as an emergency room physician. This would allow the doctor to access emergency room charts and other information required while on duty. When the physician returns to his normal department, he would access the system using his permanent role as a department chair in the obstetrics ward. This would allow him access to patient information within his department only.

Identity Manager implements NIST Level 3 RBAC. Level 3 RBAC is defined as an access control system that provides user-role review, role hierarchies, and separation constraints.

- **Level 1 RBAC**, or Core RBAC, introduces the basic concept of RBAC, where users are assigned to roles, permissions are assigned to roles, and users acquire permissions by being members of roles.
- **Level 2 RBAC**, or hierarchical RBAC, adds requirements for supporting role hierarchies. A hierarchy recognizes the concept of senior roles, which acquire the permissions of their juniors, and junior roles, which acquire the user membership of their seniors.
- **Level 3 RBAC** adds the concept of separation of duty. This concept holds that situations of conflict of interest may arise in a role-based system, where a user may gain authorization permission associated with conflicting roles, for example, accounts payable and accounts receivable. Systems implementing Level 3 RBAC enforce a static separation of duty through the enforcement of constraints on the assignment of users to roles.

Effective Account Management

Critical to implementing safeguards to meet HIPAA privacy and security requirements is an effective approach for dynamically managing the many accounts and account privileges required to give access to those who need it and deny access to those who do not need access. Identity Manager provides account administrators with an effective environment for controlling and enforcing HIPAA privacy and security rules through effective account management. This can be seen by examining the full lifecycle of the account.

- **Account Discovery.** Identity Manager provides patented mechanisms by which the administrator can understand what accesses already exist on IT systems and applications. An essential element of effective account management is the ability to model the current access rights, analyze them, detect exceptions to corporate policies, and detect and reconcile changes as they occur going forward.
- **Account Management Workflow.** The processes by which accounts are requested, approved, created, modified, and deleted are important elements of account management. The business processes controlling account creation (or “workflow”) can be automated and enforced through Identity Manager. This workflow enforcement of account creation governs the way in which accounts are requested, the approvals required for account creation, and even enforces certain restrictions on accounts. For example, Identity Manager workflow controls can restrict an individual from obtaining accounts on the accounts payable and accounts receivable systems, thus enforcing the separation of duty principle.
- **Delegated Administration.** Closely associated with workflow, delegated administration is the ability for people outside IT, even end users, to request additions, changes, and deletions to accounts and access permissions. This is facilitated by the workflow and associated business rules so that no HIPAA violations regarding the management of PHI occur. Additionally, this requires a robust and granular authorization model like that found in Identity Manager.

- **Access Revocation.** Identity Manager provides the ability to control account privileges through revocation of access rights and monitoring for any changes made outside of the interface. When an individual no longer requires access to PHI, using the Identity Manager interface, the data owner may completely revoke access rights on all accounts associated with that individual. Furthermore, account privilege modifications that are made outside of the Identity Manager interface are automatically canceled and accounts are reset to the intention of the data owner within Identity Manager. Directory Server Enterprise Edition further supports access revocation through its ability to deny access based on IP address, group membership, and other criteria.
- **Centralized Resource View.** The way in which data is viewed is critical to the proper management of PHI. For example, Identity Manager provides the data owner or the auditor with a “resource view” of who has access to the information they need to protect, as well as a “user view” that details each user’s privileges.
- **Comprehensive Reporting.** Identity Manager provides regular reporting of accounts and account privileges. Typical reports generated include the presence of dormant accounts on different IT systems and applications, aged or stale passwords, and changes to account attributes and privileges.

Reasonable Safeguards

HIPAA privacy regulations require reasonable administrative, physical, and technical safeguards. Considering the complex and dynamic environment of large organizations, “reasonable safeguards” should include technical tools to ensure that PHI access is consistent with established policies and procedures.

- **Automation.** Identity Manager automates the process of account creation, modification, and deletion. In addition to the workflow capabilities previously mentioned, Identity Manager can integrate directly into an HR system or any other authoritative system to get some or all of a user’s information. This integration, combined with business logic, allows for changes about a user to be propagated with or without human intervention to any or all IT systems or applications.
- **Customized Views.** With Identity Manager, different administrators, supervisors, and users can have different “views” of the same account information. For example, one person may access a user’s records and see test results without seeing the person’s name. Another person may access a person’s profile information without seeing any medical information. Custom views enable people to see only the data they are authorized to see and blocks data for which they are unauthorized to see.
- **Policy Enforcement.** Identity Manager provides a robust rules engine that encapsulates the required organizational policies and safeguards so that all account management is performed consistently with those policies.
- **Auditing.** Identity Manager maintains a complete audit log of all account management activities performed. Directory Server Enterprise Edition provides audit logging that can be used to determine who accessed what and when, along with scripts that process these logs to create reports. Access Manager enables the enterprise to audit all access activities, including authentication attempts, authorizations, and changes made, to assist in complying with regulatory audit requirements.

Termination Procedures

HIPAA security regulations call for the establishment of effective termination procedures to include changing of locks, removal of access from lists and all user accounts, and retrieval of tokens and access cards.

Identity Manager provides effective tracking of all accesses to PHI for each individual. Such accesses can be user accounts on various systems and under various names, and company issued equipment such as tokens and access cards. More importantly, Identity Manager can instantly and securely deprovision a user when they leave or change roles within an organization.

Entity Authentication

HIPAA security regulations call for effective entity authentication. This should include automatic logoff of accounts, unique user identification, strong passwords, and two-factor authentication. Access Manager provides authentication and policy-based authorization with a single, unified framework for securing the delivery of essential identity and application information. By utilizing a central point of authentication, role-based access control (RBAC), and single sign-on (SSO), Access Manager provides an effective and scalable security model across all Web-based applications. This eases the exchange of information and transactions while protecting the privacy and security of vital identity information.

Access Manager supports the latest federation standards — Liberty Alliance Phase 2 and SAML 1.1 specifications — to allow single sign-on across heterogeneous IT environments, including Microsoft Windows Desktop environments, through the Kerberos authentication module. By eliminating the need for proprietary and redundant security code in each application, Access Manager makes a difference in the company's bottom line by significantly reducing administrative costs and application development time.

Password Strength Enforcement

Identity Manager enforces password strength policies throughout multiple systems. This helps to ensure that the existing identification and authentication mechanisms are used effectively and according to organizational policies.

- **Two-factor Authentication Support.** Identity Manager integrates with multiple authentication mechanisms to provide for strong authentication. Rules can be created to force two-factor authentication for accounts with access to specific information.

Chapter 4

Implementation of Identity Management Systems

It is clear from the previous discussions that an identity management system (IMS) is essential in large organizations to effectively implement a HIPAA-compliant solution. However, the implementation of an IMS in an existing enterprise across multiple systems and even organizations is not without its challenges. Many IMS integration efforts find it difficult to deploy the IMS and retain existing business processes. With Sun's identity management solutions, these challenges become easier to overcome with the following capabilities:

- **Leverage Existing Data Structures.** Unlike Sun identity solutions, other IMS products create additional copies of the existing data structures in order to model and then manage account information. This adds additional PHI, requires additional controls, and unnecessarily complicates HIPAA compliance efforts.
- **Ease of Use.** Many IMS products can complicate business operations through additional work-arounds, training, and processes to fit the IMS into the organizational processes, and may require changes in existing business processes. Organizations that have developed workflows, business processes, and even scripts for implementing many account provisioning procedures will need to redesign their processes to adapt to the available processes within the deployed IMS.
 - Other solutions may lose integrity of accounts if platform interfaces are ever used. Organizations will need to develop additional procedures to ensure account integrity.
 - Many IMS products require account administrators and managers to learn a new interface with new commands, screens, and reports. Organizations implementing these systems will need to provide training to administrators and managers for new interface, controls, and reports.

The following table represents the safeguards (administrative, physical, and technical) required for HIPAA compliance and illustrates the areas in which Sun's identity management products can assist in HIPAA compliance.

HIPAA Regulation Element	Sun Solution	Sun Identity Management Capabilities
Access Controls	Access Manager	• Ensures that all appropriate authentication credentials are required of users, depending on the value of the protected resources
	Directory Server Enterprise Edition	• Supports access revocation through access denial based on IP address, group membership, and specific criteria

HIPAA Regulation Element	Sun Solution	Sun Identity Management Capabilities
	Identity Manager	<ul style="list-style-type: none"> • Implements structured access control techniques, such as “NIST Level 3 RBAC” • Provides centralized authentication and authorization capabilities • Controls access based on specific criteria and intercepts unauthorized operations
Audit Controls	Directory Server Enterprise Edition	<ul style="list-style-type: none"> • Provides audit logging, which can be used to determine who accessed what and when, along with scripts that process these logs to create reports
	Identity Manager	<ul style="list-style-type: none"> • Provides comprehensive account review and reporting on current permissions (both from a resource perspective and from a user perspective)
	Access Manager	<ul style="list-style-type: none"> • Offers audit support of the identity entitlement infrastructure, enabling administrators to know not only who has access to what currently, but also who had access to what in the past
Authorization Controls	Access Manager	<ul style="list-style-type: none"> • Delivers decentralized authentication and authorization services across internal and external computing domains and ensures that authorized users have access to specific resources while protecting those resources from unauthorized users
	Identity Manager	<ul style="list-style-type: none"> • Provides effective tools for account administrators to enable, modify, and disable user permissions to view and edit personal health information (PHI) • Delivers dynamic privilege extensions (emergency access) through dynamic predefined rules • Automates effective termination procedures • Enforces approval processes for the granting of modifications to and revocation of access privileges • Enforces security policies, such as authentication controls, permission expiration controls, and password hardness policies
Data Authentication	Identity Manager	<ul style="list-style-type: none"> • Offers workflow process to enforce multiple reviews prior to accepting data entry
Entity Authentication	Identity Manager	<ul style="list-style-type: none"> • Provides two-factor authentication support, including ID/Password, PKI certificates, ID tokens, and biometrics
Message Authentication	Identity Manager	<ul style="list-style-type: none"> • Includes digitally-signed e-mail for approval processing and digitally-signed transactions/workflows to ensure end-to-end authentication
Alarm/Notification	Identity Manager	<ul style="list-style-type: none"> • Notifies and automates action on out-of-compliance security policy enforcement, such as password expirations, orphan accounts, and separation of duty conflicts

HIPAA Regulation Element	Sun Solution	Sun Identity Management Capabilities
Audit Trail	Access Manager and Identity Manager	<ul style="list-style-type: none"> • Provides digitally-signed audit log of all activities — both manual and automated — to provide visibility into what activities have been executed by whom
Availability of PHI	Directory Server Enterprise Edition	<ul style="list-style-type: none"> • Ensures high availability of PHI within a secure infrastructure based on a highly scalable, centralized repository for identity, application, and network resources information • Prevents denial-of-service attacks • Ensures availability of service with failover/failback operations, allowing directory service to continue when server is offline • Outage-free maintenance allows back-end servers to be taken down for maintenance without compromising directory service

Sun provides a unified portfolio for using, sharing, and managing identity information. Sun's identity management suite provides three unique attributes that are critical to the success of any identity management solution:

1. **Open:** Enterprises today operate in heterogeneous environments, and require technology solutions that run on multiple platforms and interoperate with technologies from various vendors. Sun is a leading contributor to identity management standards, which fosters openness and interoperability within the products and helps to protect existing and future technology investments.
2. **Secure:** Sun's identity management product line delivers a single point of control for managing user lifecycles and entitlements with centralized policy enforcement:
 - Protection for enterprise resources from unauthorized access
 - Reduction in risk of security breaches
 - Easier to comply with legislative mandates such as HIPAA
3. **Unified:** Sun identity management solutions deliver a comprehensive, holistic approach to managing identities, credentials, and policy across application and organizational boundaries, resolving the overlaps and inconsistencies resulting from multiple identity repositories and policy frameworks.

Chapter 5

Sun Identity Management: A Key Component for HIPAA Compliance

While implementation of a single technology or mechanism cannot completely meet HIPAA privacy and security regulations, the functions, features, and capabilities of Sun's identity management solutions are essential to implementing a HIPAA-compliant operation within organizations — large or small — that exchanges individually identifiable health information, including entities such as:

- Payers
- Providers
- Clearinghouses
- Laboratories
- Billing agencies
- Pharmaceutical and biotechnology companies

Sun's identity management solutions implement many required elements of HIPAA privacy and security regulations. For large organizations, the implementation of these elements requires the use of technology — such as Sun's identity management products — that can efficiently and effectively automate and enforce these elements.

About Sun

Since its inception in 1982, customers have continually turned to Sun to help them grow their business, lower their costs, and gain competitive advantage. Sun is a leading provider of industrial-strength hardware, software, services, and technologies that make the Net work.

Sun's identity management products provide a complete, end-to-end offering that reduces cost and complexity, and scales to meet the growing requirements of enterprises and service providers. With a proven ROI track record for Fortune 500 organizations, Sun delivers real business value through innovative solutions that give organizations a competitive advantage.

For more information, visit sun.com/identity_mgmt.

© 2004 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, CA 95054 USA

All rights reserved.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any. Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California.

Sun, Sun Microsystems, the Sun logo, Java, and The Network is the Computer are trademarks, registered trademarks, or service marks of Sun Microsystems, Inc. in the U.S. and other countries.

UNIX is a registered trademark in the United States and other countries, exclusively licensed through X/Open Company, Ltd.

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

RESTRICTED RIGHTS: Use, duplication, or disclosure by the U.S. Government is subject to restrictions of FAR 52.227-14(g)(2)(6/87) and FAR 52.227-19(6/87), or DFAR 252.227-7015(b)(6/95) and DFAR 227.7202-3(a). DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS HELD TO BE LEGALLY INVALID.



Please
Recycle



Adobe PostScript

Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA Phone 1-650-960-1300 or 1-800-555-9SUN Web sun.com



Sun Worldwide Sales Offices: Argentina +5411-4317-5600, Australia +61-2-9844-5000, Austria +43-1-60563-0, Belgium +32-2-704-8000, Brazil +55-11-5187-2100, Canada +905-477-6745, Chile +56-2-3724500, Colombia +571-629-2323, Commonwealth of Independent States +7-502-935-8411, Czech Republic +420-2-3300-9311, Denmark +45 4556 5000, Egypt +202-570-9442, Estonia +372-6-308-900, Finland +358-9-525-561, France +33-134-03-00-00, Germany +49-89-46008-0, Greece +30-1-618-8111, Hungary +36-1-489-8900, Iceland +354-563-3010, India-Bangalore +91-80-2298989/2295454; New Delhi +91-11-6106000; Mumbai +91-22-697-8111, Ireland +353-1-8055-666, Israel +972-9-9710500, Italy +39-02-641511, Japan +81-3-5717-5000, Kazakhstan +7-3272-466774, Korea +82-2193-5114, Latvia +371-750-3700, Lithuania +370-729-8468, Luxembourg +352-49 11 33 1, Malaysia +603-21161888, Mexico +52-5-258-6100, The Netherlands +00-31-33-45-15-000, New Zealand-Auckland +64-9-976-6800; Wellington +64-4-462-0780, Norway +47 23 36 96 00, People's Republic of China-Beijing +86-10-6803-5588; Chengdu +86-28-619-9333, Guangzhou +86-20-8755-5900; Shanghai +86-21-6466-1228; Hong Kong +852-2202-6688, Poland +48-22-8747800, Portugal +351-21-4134000, Russia +7-502-935-8411, Saudi Arabia +9661 273 4567, Singapore +65-6438-1888, Slovak Republic +421-2-4342-94-85, South Africa +27 11 256-6300, Spain +34-91-767-6000, Sweden +46-8-631-10-00, Switzerland-German 41-1-908-90-00; French 41-22-999-0444, Taiwan +886-2-8732-9933, Thailand +662-344-6888, Turkey +90-212-335-22-00, United Arab Emirates +9714-3366333, United Kingdom +44 0 1252 420000, United States +1-800-555-9SUN or +1-650-960-1300, Venezuela +58-2-905-3800, or online at sun.com/store

SUN © 2004 Sun Microsystems, Inc. All rights reserved. Sun, Sun Microsystems, the Sun logo, Java, and The Network is the Computer are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. Information subject to change without notice. 09/04 R1.0