

# CONSOLE *WORKS* SUPPORT FOR HIPAA COMPLIANCE

VERSION INFORMATION: 09/23/2002

INTENDED AUDIENCE: HEALTHCARE PROVIDERS  
INFORMATION SYSTEMS PROFESSIONALS  
INFRASTRUCTURE SECURITY PROFESSIONALS

## ABSTRACT:

The Health Insurance Portability and Accountability Act (HIPAA) was signed into federal law in 1996 Public Law 104-191. While the primary intent and purpose of this law is to protect health insurance coverage for workers and their families when they change or lose their jobs, the various provisions have far-reaching impact on healthcare transactions and the administrative information systems. ConsoleWorks provides controlled access, auditing information and complete logging for critical healthcare systems. This document addresses the applicability of a ConsoleWorks implementation in the health care space.

Copyright (c)2002 TECSys Development LP.

Printed in the United States of America.

TECSys Development, LP (TDi) makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, TDi reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of TDi to notify any person of such revision or changes.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means electronic, mechanical, magnetic, optical, chemical, or otherwise without the prior written permission of:

TECSys Development, LP	Phone: 972.881.1553
1600 10th Street	FAX: 972.424.9181
Suite B	Email: <a href="mailto:support@tditx.com">support@tditx.com</a>
Plano, TX 75074 USA	web: <a href="http://www.tditx.com/">http://www.tditx.com/</a>

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 52.227-7013.

TECSys Development and ConsoleWorks are trademarks of TECSys Development, LP.

All product or company names mentioned in this document are trademarks or registered trademarks of their respective owners.

All Rights Reserved.

# ConsoleWorks Support for HIPAA Compliance

## Background

The Health Insurance Portability and Accountability Act (HIPAA) was signed into federal law in 1996 Public Law 104-191. HIPAA requires the Secretary of the Department of Health and Human Services (HHS) to adopt standards for electronic transactions, including data elements, standard code sets, unique health identifiers, security safeguards and privacy standards.

The primary intent and purpose of this law is to protect health insurance coverage for workers and their families when they change or lose their jobs. It was recognized that this new protection would impose additional administrative burdens on health care providers, payers and clearinghouses; and therefore, the law includes Section 262, Administrative Simplification. This section is specifically designed to reduce the administrative burden associated with the electronic transfer of health information between organizations, and more generally, to increase the efficiency and cost-effectiveness of the United States health care system. This approach accelerates the move from certain paper-based administrative and financial transactions to electronic transactions through the establishment of national standards.

The HHS has issued a series of guidance materials on the federal privacy protections for medical records and other personal health information. This guidance explains and clarifies key provisions of the medical privacy regulation, which was published earlier. Providing this guidance is part of an ongoing process to help health care providers and health plans come into compliance with the regulation by April 14, 2003.

## Introduction

Signed into law by President Clinton on August 21, 1996, HIPAA offers new protections for millions of American workers that improves portability and continuity of health insurance coverage.

HIPAA protects workers and their families by:

- Limiting exclusions for preexisting medical conditions;
- Providing credit for prior health coverage and a process for providing certificates concerning prior coverage to a new group health plan or issuer;
- Providing new rights that allow individuals to enroll for health coverage when they lose other health coverage or add a new dependent;
- Prohibiting discrimination in enrollment and in premiums charged to employees and their dependents based on health status-related factors; guarantees availability of health insurance coverage for small employers and the ability to renew health insurance coverage in both the small and large group markets; and preserves the states' role in regulating health insurance, including the states' authority to provide greater protections.
- Preexisting Condition Exclusions

The law defines a preexisting condition as one for which medical advice, diagnosis, care, or treatment was recommended or received during the six-month period prior to an individual's enrollment date. Most group health plans may not exclude an individual's preexisting medical condition from coverage for more than 12 months (18 months for late enrollees) after an individual's enrollment date.

Under HIPAA, a new employer's plan must give individuals credit for the length of time they had continuous health coverage, thereby reducing the 12-month exclusion period. Individuals who have 12 months of continuous health coverage - without a break in coverage of 63 days or more - do not have to start over with a new 12-month exclusion for any preexisting conditions.

## Administrative Simplification

HIPAA's "Administrative Simplification" provision is composed of four parts, each of which have generated a variety of "rules" and "standards."

The four parts of Administrative Simplification are:

I. **ELECTRONIC HEALTH TRANSACTIONS STANDARDS**—The term "Electronic Health Transactions" includes health claims, health plan eligibility, enrollment and dis-enrollment, payments for care and health plan premiums, claim status, first injury reports, coordination of benefits, and related transactions. Today, health providers and plans use many different electronic formats. Implementing a national standard will simplify and improve transaction efficiency nationwide. Virtually all health plans will adopt these standards, even if a transaction is on paper, by phone or by FAX. Providers using non-electronic transactions are not required to adopt the standards; although if they don't, they will have to contract with a clearinghouse to provide translation services.

II. **UNIQUE IDENTIFIERS FOR PROVIDERS, EMPLOYERS, HEALTH PLANS and PATIENTS** - The current system allows us to have multiple ID numbers when dealing with each other. HIPAA sees as confusing, conducive to error and costly. It is expected that standard identifiers will reduce these problems.

III. **SECURITY OF HEALTH INFORMATION & ELECTRONIC SIGNATURE STANDARD** - The new Security Standard will provide a uniform level of protection of all health information that is housed or transmitted electronically and that pertains to an individual. In addition, organizations who use Electronic Signatures must meet a standard ensuring message integrity, user authentication, and non-repudiation. The Security standard mandates safeguards for physical storage and maintenance, transmission, and access to individual health information. This applies not only to the transactions adopted under HIPAA, but to all individual health information that is maintained or transmitted.

IV. **PRIVACY AND CONFIDENTIALITY** - The Final Rule for Privacy was published just as President Clinton was leaving office. In general, privacy is about who has the right to access personally identifiable health information. The rule covers all individually identifiable health information in the hands of covered entities, regardless of whether the information is or has been in electronic form.

Accountability is a key issues for all involved and governed by HIPPA. For the first time, there will be specific federal penalties if a patient's right to privacy is violated. Therefore, assessment, analysis, and compliance programs are necessary to ensure an organization has taken the proper steps for the future.

## The AFEHCT

The Association for Electronic Health Care Transactions (AFEHCT) is dedicated to supporting the use of EDI to improve and reduce the cost of health care. This industry group is:

- Dedicated to effectively addressing detailed issues to meet the challenges of Health Care EDI
- Addressing technical and policy issues and is a recognized leader by government healthcare and legislative organizations
- Recognized in Washington as the PRO-ACTIVE Health Care EDI Industry Association

The goals of the organization include administrative simplification and cost reduction; the creation of open markets and health industry competition; addressing threats that would challenge the industry's free enterprise; working with the appropriate agencies to establish Privacy and Security standards for patient data; and providing a forum for vendors, payors and providers to work together to reduce the cost and improve the quality of health care through electronic data interchange (EDI).

Initiatives supported by the AFEHCT cover a number of the disciplines necessary to the successful implementation of and adherence to the HIPAA regulation. Examples include:

#### Projects

- Work with HCFA to modify policies and procedures to simplify and reduce the cost of Medicare and Medicaid EDI.
- Work with HCFA and DHHS to implement administrative simplification as stated in the HIPAA Legislation.
- Develop and present recommendations for regulatory requirements for administrative simplification, privacy and security.
- Review NPRMs and develop responses.
- Testify before Congressional committees on health care issues.
- Education and Accreditation Programs.

#### Work Groups

- Medicare/Medicaid EDI
- Update HCFA EDI Support Manual for Medicare.
- Identify and Prioritize Issues and Concerns regarding Medicare and Medicaid EDI and report to HCFA.
- Address HCFA Medicare Data Network issues.

#### Administrative Simplification

- Identify Issues and Implementation Concerns regarding HIPAA Standards.
- Establish on-going recommendations for health care industry transaction implementation formats and guides.
- Work to establish Payor Ids, Provider Ids and Patient Ids.

#### Security Work Group

- Define security and risk levels for the health care industry.
- Work with HCFA and DHHS to establish Security Measures based on Risk Levels.

#### Privacy Work Group

- Establish what information must be protected and when encryption or digital signatures are required.
- Coordinate industry input for national and state patient privacy legislative issues.

In summary, the AFEHCT is quite busy addressing the assisting the community to deal with and ensure compliance with all the critical aspects of the HIPAA regulations.

## **What is ConsoleWorks and How can it Help?**

ConsoleWorks is an out-of-band enterprise-class systems and network management software tool that provides you with direct access to systems and network device consoles. Unlike conventional in-band tools that depend on the Simple Network Management Protocol (SNMP), ConsoleWorks relies on direct system connections and real-time data collection. This means that the environment is much easier to implement, does not rely on the network for operation, and is not subject to the current wave of SNMP denial of service attacks.

ConsoleWorks may be hosted on a variety of platforms and operating systems which enables data center managers to leverage existing expertise. It continually monitors all system error and information codes reporting issues immediately for quick response. Existing users confirm that ConsoleWorks strengths are:

- 1) Active Monitoring and Alerting**
- 2) Direct Console Access from Anywhere, at Anytime**
- 3) Complete Logging of All Console Communication**
- 4) Knowledge Base and Content Sensitive Help**
- 5) Enhanced Security**

Active monitoring of all system and device consoles and real-time notification helps ensure system uptime. The ability to receive messages that often go unnoticed, provides operations personnel the ability to respond most often before system issues affect actual performance.

Direct access from anywhere, at any time allows the operations staff to get to the problem immediately regardless of staff location. This means quick response to system needs without delay and which helps maximize overall uptime.

The logs maintained by *ConsoleWorks* provide a complete history and audit trail for each managed device. They not only provide the necessary data for system support, but also serve a 'complete' history of the system's activity.

*ConsoleWorks*' configuration information and context sensitive help record your environment and present this information to system operators for rapid review. During operations, *ConsoleWorks* allows existing information to be updated and supplemental data to be collected for rapid recall. This ongoing process puts critical data the fingertips of staff, facilitating rapid return to operation after system issues occur.

*ConsoleWorks* runs 24x7 without a break. During that time, it will monitor and manage all the machines connected to it, whether the connections are its own or a device managed by another *ConsoleWorks* server. *ConsoleWorks* can monitor and manage any machine that has a console port or supports Serial, Telnet, Syslog, or LAT connections. In short, *ConsoleWorks* can manage just about any computer or network based device made in the last 20 years. Because it uses out-of-band management, *ConsoleWorks* provides a user the capability to verify current status using real-time data, troubleshoot the machine regardless of the operating system health (no agent needed), and even restart the machine remotely. *ConsoleWorks* actions can be configured to notify (Email, phone, page, etc.) personnel for any situation at any time using any means available to the *ConsoleWorks* server. Since *ConsoleWorks* can be configured to engage its automatic actions at any time, it is like having an around-the-clock faithful and dedicated operator watching your environment and alerting you when important events occur.

## **ConsoleWorks Events and Scan Files**

*ConsoleWorks* events are based on text matching for specific data. This process allows users to easily create alerts based on their specific environment. Whether it be a application, a system, or a security issue; *ConsoleWorks* provides realtime notification in order to address immediate action.

Scan files are *ConsoleWorks* data modules for specific devices or systems. They contain lists of information, error codes, and corrective actions as identified by the device's manufacturer. The lists are compiled into *ConsoleWorks* event and scan formats. *ConsoleWorks* then uses the events from these scan files to monitor devices as directed in the device's configuration screen.

## **The Security Checklist**

The AFEHCT Security Work Group has gathered a Security Self-Evaluation Checklist to help organizations affected by the HIPAA Act of 1996 in evaluating their compliance with the Security requirements of the Administrative Simplification section. Specifically, it addresses areas of security which fit under the requirements of Section 1173 (d) and (e) , concerning "Security Standards for Health Information" and "Electronic Signature".

If an organization plays multiple roles, such as selling software to different portions of the industry, and offering EDI services, then they may need to complete the assessment more than once, so that each role is represented independently. It is important for each entity within the industry to perform a Security self evaluation, in order to determine their level of security with regard to the requirements of HIPAA.

The checklist is organized following the recommendations from the National Committee on Vital & Health Statistics to the Secretary of the Department of Health and Human Services, dated September 9, 1997. The AFEHCT Security Work Group developed this checklist from "For the Record: Protecting Electronic Health Information" by the National Research Council, the HI-

PAA Security Matrix from the DHHS, and other sources.

This Checklist is only a tool to assist in the self-evaluation, and it is NOT a guarantee of compliance, nor a listing of security requirements for compliance. The sections that follow match ConsoleWorks functionality to the Security Checklist in order to provide a basis for HIPAA compliance.

## Section 1. Individual Authentication of Users

<u>Description</u>	<u>ConsoleWorks Support</u>	<u>Note</u>
Unique individual identifier for each user	Yes	ConsoleWorks users have a unique account requiring a username and password for accessing the system
Automatic logoff after specified time	Yes	Configurable
Change passwords often (enforced by system)	Yes	Configurable
System generates random password	No	Not for user accounts
Weak passwords not allowable	No	Recommended
System stores password encrypted	Yes	
Uniform User ID across organization	Optional	ConsoleWorks supports RADIUS of LDAP for single user identification
Incentives to reduce key account sharing	N/A	Recommended in site security policy
Single-use or token based passwords	Optional	ConsoleWorks supports RADIUS of LDAP for single user identification
Token card plus password or PIN	Capability Exists	Can be supported by 3rd party using ConsoleWorks API
Biometric (fingerprint, retinal scan, etc.)	Capability Exists	Can be supported by 3rd party using ConsoleWorks API
Caller-ID verification of remote location	N/A	
Telephone callback for remote users	N/A	
Different security for terminals in different locations	No	Possible
Comply with Orange Book C2 or better	No	
Account canceled when employee leaves	Not Automatic	Recommended for security policy
Emergency access procedures for forgotten password	Yes	System Administrator
Policies and procedures in place for Authentication	Yes	ConsoleWorks supports this feature
Policies and procedures strictly enforced (even fines)	N/A	—

## Section 2. Access Control

<u>Description</u>	<u>ConsoleWorks Support</u>	<u>Note</u>
Access control lists for each file or database	Yes	ConsoleWorks logs all access and activity related to its database. Managed systems can be configured to report database related access to ConsoleWorks to provide a single point for audit trails.
Access control lists UserID based	Yes	ConsoleWorks logs activity based on user and activity. Managed systems can be configured to report user activity to ConsoleWorks to provide a single point for audit trails.
Role based access profiles	Yes	Profiles within ConsoleWorks grant privileges necessary to interact with the consoleWorks configuration and/or the individual managed devices
Access overrides for emergencies	Yes	ConsoleWorks administrative account
Simple access control (or nothing)	Yes	Selectable profiles for access level changes
Gross granularity control (record based, or role based algorithm)	Yes	Through ConsoleWorks profiles
Medium granularity control (record based, or role based algorithm)	Yes	Through ConsoleWorks profiles
Medium granularity control (record based, or role based algorithm)	Yes	Through ConsoleWorks profiles
Multiple parameters (e.g. UserID, role, physical location, function, etc.)	Yes	Using ConsoleWorks account and profiles.
Policies and procedures in place fo Access Control, and to determine legitimate need	Indirectly	Through ConsoleWorks profiles
Policies and procedures strictly enforced (even fines)	N/A	—

## Section 3. Monitoring of Access

<u>Description</u>	<u>ConsoleWorks Support</u>	<u>Note</u>
System imposed audit trails	Yes	ConsoleWorks logs all activity reported from applications, managed systems, and security controls.
Software controlled audit trails	Yes	ConsoleWorks provides an audit trail for all activity related to console/device management
Transaction log audit trail	Yes	By database configuration to report to ConsoleWorks
Record level audit trail	Yes	By database configuration to report to ConsoleWorks
Field level audit trail	Yes	By database configuration to report to ConsoleWorks
Write or change data audit trail	Yes	By system/database configuration to report to ConsoleWorks
Read, display, print data audit trail	Yes	By system/database configuration to report to ConsoleWorks
Automatic display of "last access" to the next user, to allow self-audit by all users	Indirectly	ConsoleWorks provides user audit trail in the log files which may be reviewed
Periodic management reports of exceptions	Yes	ConsoleWorks provides capability to produce custom reports
Period management reports of all access	Yes	ConsoleWorks provides capability to produce on-demand access reports
Internal periodic audit of audit trails	Yes	ConsoleWorks provides capability to produce audit reports on a scheduled basis
Policies and procedures in place for Access Monitoring, to detect misuse and violations	N/A	
Policies and procedures strictly enforced (even fines)	N/A	
External/independent audit of audit trails	Yes	ConsoleWorks provides ad-hoc reporting for independent audits

## Section 4. Physical Security and Disaster Recovery

<u>Description</u>	<u>ConsoleWorks Support</u>	<u>Note</u>
Secure computer room	Partially	ConsoleWorks provides remote access capability which does not require physical computer room access.
Secure access to displays and printers	N/A	
Network security, no external network access	Yes	By managing network devices, ConsoleWorks can monitor and alerts on access and/or configuration changes.
Secure destruction of printouts, floppies, etc.	N/A	
Secure destruction of equipment	N/A	
Secure backup, storage and retrieval	N/A	
Multiple backup sites	Yes	An option within ConsoleWorks provides for automatic failover and redundant site operation.
Disaster recovery plan in place	N/A	Highly recommended
Disaster recovery plan periodically tested	N/A	Highly recommended
Emergency data access assured in case of disaster	Yes	Since ConsoleWorks provides access from 'anywhere at anytime', remote personnel can assure system/network functionality
Data content integrity assured	N/A	
Operations recoverability	Yes	Since ConsoleWorks provides access from and logs necessary for recovery
No-disruption of critical functions	Yes	Access from 'anywhere at anytime' assures continuous operation
Policies and procedures in place for Physical Security and Disaster Recovery	N/A	
Policies and procedures strictly enforced (even fines)	N/A	
Security maintained 100% in disaster recovery mode	Yes	ConsoleWorks performs in recovery mode the same as in normal operation ensuring access and maintaining audit trails.

## Section 5. Protection of Remote Access Points and Protection of External Electronic Communications

<u>Description</u>	<u>ConsoleWorks Support</u>	<u>Note</u>
Firewall for Internet access	Supports	ConsoleWorks can manage and collect data from firewalls providing a single point for data collection
Encrypted Virtual Network for Internet	Yes	ConsoleWorks supports encryption techniques for data communication
Limit use of the Internet to USA remote sites	Supports	Network devices and configurations can be managed using ConsoleWorks and alerts established for access violations and configuration changes
Healthcare data available to external network	N/A	
Strong encryption required for Internet and Extranet users	Yes	ConsoleWorks supports encryption techniques for data communication
Authentication and Digital signatures required for Internet and Extranet users	Yes	ConsoleWorks supports authentication for encrypted sessions
Dial-In protections (e.g. Caller-ID, callback, encryption)	N/A	
Mobile access (laptop/handheld) physical protection and data encryption	Yes	ConsoleWorks supports encryption techniques for mobile data communication
Healthcare data over Infrared or Radio links encrypted and authenticated	Yes	ConsoleWorks supports encryption techniques for radio link communication
Control IP addresses, prevent IP spoofing	N/A	

## Section 6. Software Discipline

<u>Description</u>	<u>ConsoleWorks Support</u>	<u>Note</u>
Virus checking all files	N/A	
Virus checking electronic mail	N/A	
Control or restrict user software	N/A	
Control PC software loading	N/A	
Network software periodic census	Yes	For devices managed by ConsoleWorks
Version control / Change control in use	N/A	
Policies and procedures in place for assurance and software discipline	N/A	
Policies and procedures strictly enforced (including fines)	N/A	
Periodic user training on required procedures	N/A	

## Section 7. System Assessment

<u>Description</u>	<u>ConsoleWorks Support</u>	<u>Note</u>
Run anti-virus programs	Yes	Through 'scheduled actions' ConsoleWorks can direct systems to run applications.
Vulnerability evaluation	N/A	
Stay up on CERTS alerts	N/A	
Avoid or update obsolete technologies	N/A	
Network software periodic census	Yes	ConsoleWorks can be configured to provide this information
Version control / Change control in use	N/A	ConsoleWorks provides a repository for this type information
Policies and procedures in place for system self-assessment evaluation	N/A	
Policies and procedures strictly enforced (even fines)	N/A	

## Section 8. Monitoring of Integrity of Data

<u>Description</u>	<u>ConsoleWorks Support</u>	<u>Note</u>
Document integrity checking system	N/A	
Digital signatures applied to documents	N/A	
Monitor integrity of backup media	N/A	
Encrypt/sign database contents	N/A	
Checksum or signature protection of critical files	Supports	ConsoleWorks can record system events related to critical files
Policies and procedures in place for monitoring integrity of data	N/A	
Policies and procedures strictly enforced (even fines)	N/A	

## Section 9. Organizational Practices

Description	ConsoleWorks Support	Note
Scalable confidentiality and security procedures	Supports	ConsoleWorks logs all activity providing support for operational plans and procedures
Security / confidentiality committees	N/A	
Designation of an information security officer in the organization	N/A	
Education and training programs for all employees, medical staff, agents and contractors	N/A	
Organizational sanctions for violation of policies and procedures	N/A	
Improved patient authorization forms for disclosure of health information	N/A	
Patient access to audit logs	Yes	If required
Awareness training for all personnel, including management	N/A	
Written security policies and documentation	N/A	
Signed statement by all employees regarding confidentiality of records	N/A	
Defined escalation procedures, including contact names and numbers, for security issues	Partially	ConsoleWorks provides for capturing pertinent information regarding consoles, users, and events.
Personnel clearance procedure	N/A	