



CRESCENDO SECURITY

The Crescendo suite of document creation and management solutions can help your organization ensure data confidentiality with their integrated security features. Security options offered by Crescendo solutions include password controls, application security, system tracking, remote security, encryption and electronic and biometric signatures.

SYSTEM CONTROLS

Crescendo applications are equipped with integrated security features to ensure data confidentiality. All applications require a unique user login and password in order to gain access to the system. Complete with extensive privilege setting options, the system allows functions to be enabled and restricted based on user rights, ensuring each user will only have access to data on a need to know basis.

APPS SECURITY. The Crescendo Wide Area Service sets up a client-server architecture and authenticates each user connecting to the system. CWAS users access all commonly used data locally while all sensitive data is maintained on the central database, never storing confidential information on a local PC.

UNATTENDED LOGOUT. Crescendo's log out feature ensures that computers running Crescendo applications remain inaccessible if left unattended, ensuring patient data is never compromised. If left unattended for a predetermined amount of time, the user must log in once again to gain access, therefore restricted information is never viewed at an unattended workstation.

SYSTEM TRACKING. Crescendo takes data confidentiality seriously, which is why all applications come equipped with complete audit trails and logs. In the event of a data breach or leak, a system administrator can easily view detailed logs including all accesses made to a report, including who viewed, modified or printed a document. Furthermore, audit trail management reports display critical information to track system activities. The administrator can even pull up a history report which provides an instant summary of all accesses made per user or per subject.

ENCRYPTION

Crescendo ensures maximum protection against unwarranted access to files and databases through the use of hash algorithms, checksums and the Microsoft 40-bit encryption mechanism. In addition to protection for files within the system, any documents that are transferred electronically are protected as well and cannot be opened, changed or interpreted by unauthorized users.

ELECTRONIC SIGNATURE

An electronic signature carries the same legal weight as a written signature on a paper document, in accordance with HIPAA, Crescendo has established measures to ensure maximum security when electronically authenticating a document. The HIPAA mandate calls for message integrity, non-repudiation and user authentication, all of which Crescendo applications comply with.

Once a user has electronically signed a document by entering their unique personal identification number, the report is then locked. Crescendo encryption ensures the document can not be tampered with and remains intact. After this point, additions can be made to the report however these will be appended to the original signed document, with time and date stamps to denote the changes. The author PIN will be required after any edits to track these occurrences.

MULTIPLE SIGNERS. Multiple signatures are supported and a user can even select the next signer of a report, for example a resident can choose their staff physician and have the job routed for their review upon completion, guaranteeing a staff physician has seen the report before distribution. In compliance with HIPAA, Crescendo makes it possible to track the order of signatures, and even allows the administrator to set protocols that define the order of signature.

BIOMETRICS. Biometric signature refers to methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. Some Crescendo applications support biometric signature as a secure authentication method, saving time versus traditional electronic signature.

For more information about how Crescendo can keep your data safe please contact your Crescendo representative.



CRESCENDO
SYSTEMS

Corporate Head Office
1600 Montgolfier
Laval, Quebec H7T 0A2
CANADA
Tel: 1-800-724-2930
Fax: (450) 973-4449

Crescendo Systems Limited
Saxon House
Downside, Sunbury
Middlesex, TW16 6RT
UNITED KINGDOM
Tel: +44 (0) 1932 789433
Fax: +44 (0) 844 846 6416

Systèmes Crescendo
34 avenue des Champs
Elysées
75008 Paris
FRANCE
Tel: 08 00 90 30 12

CRESCENDO SYSTEMS CORPORATION
Tel: +1 (450) 973-8029
Fax: +1 (450) 973-4449
E-mail: info@crescendo.com

CORPORATE HEADQUARTERS
1600 Montgolfier
Laval, QC H7T 0A2
CANADA

© 2014 Crescendo Systems Corporation. All product names, brand names, company names, trademarks and registered trademarks are the property of their respective holders. Specifications are subject to change without notice.