

Deploying Hummingbird Document and Records Management Products to Comply with 21 CFR Part 11: Electronic Records; Electronic Signatures

A White Paper prepared for Hummingbird Ltd.

*By Thomas Meehan,
Director Compliance Technology
Integrated Compliance Technology, Inc.*



Transforming Information into Intelligence™

While every attempt has been made to ensure the accuracy and completeness of the information in this document, some typographical or technical errors may exist. Hummingbird cannot accept responsibility for customers' losses resulting from the use of this document. The information contained in this document is subject to change without notice.

This document contains proprietary information that is protected by copyright. This document, in whole or in part, may not be photocopied, reproduced, or translated into another language without prior written consent from Hummingbird.

This edition published April 2003

Table of Contents

Overview	5
Understanding the Rule — Electronic Records; Electronic Signatures (Part 11)	6
Hummingbird DM Meets 21 CFR Part 11 Technical Requirements for Electronic Records. . . .	9
Integrating <i>ApproveIt</i> Electronic Signature Software with Hummingbird DM Meets 21 CFR Part 11 Technical Requirements for Electronic Signatures	10
Hummingbird RM Complements Hummingbird DM to Facilitate Compliance Through Good Electronic Records Management	11
Deploying Hummingbird Products to Comply with 21 CFR Part 11	12
Validation.....	12
Product Planning	13
Product Configuration	14
Other Implementation Considerations	16
SQL Database Security	16
Written Procedures	16
System Testing.....	17
Installation Plan and Report	17
Develop and Execute Test Scripts	17
Ongoing Operation and Maintenance	18
Training Records and Qualifications	18
Configuration Management/Change Control	19
Conclusion	20
Appendix A	21
Subpart B — Electronic Records	21
Section 11.10 Controls for Closed Systems	21
Section 11.50 Electronic Manifestations	23
Section 11.70 Signature/Record Linking	23
Subpart C — Electronic Signatures	24
Section 11.100 General Requirements	24
Section 11.200 Electronic Signature Components and Controls.....	24
Section 11.300 Controls for Identification Codes/Passwords	25

Overview

In response to the increased use of electronic records to maintain information subject to FDA regulatory review, the FDA made effective 21 CFR Part 11: Electronic Records; Electronic Signatures. The rule defines the technical and procedural requirements that, when implemented, would ensure the integrity of the information contained within an electronic record throughout the record's retention period. The rule also defines the requirements for the signing of electronic records where the signature may either be an electronic signature or a physical signing that is technically linked to the electronic record.

The impact of this rule on FDA regulated industry has been widespread. Within the scope of this rule are not only the electronic records maintained within traditional databases, but also electronic records created by general business applications such as word processors, spreadsheets and computer-aided design. The leading general business applications do not provide the record management tools to adequately control the integrity and security of the electronic records that they create and modify.

The Hummingbird DM™ (Document Management) and Hummingbird RM™ (Record Management) products facilitate the proper management of non-database electronic records, enabling control of an electronic record from creation through revision, dissemination, retirement and destruction. The Hummingbird DM and Hummingbird RM product(s) can be a key component of a regulated firm's overall Part 11 compliance strategy.

This paper shall describe how Hummingbird DM and Hummingbird RM provide a framework for a comprehensive program for maintaining the integrity of non-database electronic records thereby meeting the technical requirements of 21 CFR Part 11. This paper shall also provide a roadmap for compliance, providing configuration and implementation guidance for deploying the Hummingbird products in the regulated environment.

Understanding the Rule — Electronic Records; Electronic Signatures (Part 11)

The FDA is responsible for ensuring the safety and efficacy of manufactured pharmaceuticals, biotechs, and medical devices. FDA regulated industries include pharmaceutical, biotechs, medical device, quality control laboratories, and clinical research organization. FDA's authority is international, with any company that sells regulated products into the U.S. market within their jurisdiction.

FDA has published a series of regulatory requirements in the Code of Federal Regulations (CFR) targeted at record keeping and reporting. These regulations specify the requirements for record keeping and reporting to ensure that the process used in developing, testing and manufacturing a drug or device can be reviewed. Failure to adhere to these regulations can result in the product being deemed adulterated and subject to seizure.

Over the past 20 years, much of the information covered within the record keeping and reporting requirements has migrated from paper records to electronic records. Cognizant that the process for maintaining electronic records differs greatly from paper, the FDA issued 21 CFR Part 11: Electronic Records; Electronic Signatures. This rule specified the requirements for maintaining the integrity of electronic records, and for affixing electronic signatures to these electronic records.

Since Part 11 was made effective in August 1997, the regulated industry has been struggling to bring their organizations into compliance. The rule stipulates that persons who create, modify, maintain or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity and when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Complicating compliance was the regulation's broad scope:

The rule applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted under any records requirement set forth in agency regulations. This rule also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in the agency regulation.

And the broad definition of an electronic record:

Any combination of text, graphics, data, audio, pictorial or other information representation in digital form that is created, modified, maintained, archived, retrieved or distributed by a computer system.

While the initial focus was to bring into Part 11 compliance key information systems such as Laboratory Information Management Systems (LIMS), Manufacturing Execution Systems (MES) and Manufacturing Resource Planning (MRP) systems, the FDA has recently cited industry for failure to control system diagrams and spreadsheet files as it has intensified its enforcement of the rule.

Based on the rule's scope, non-database electronic records generated by general business applications are also subject to the rule's technical and procedural requirements to include:

- Word processing files such as Standard Operating Procedures describing the manufacturing process and new drug applications.
- Spreadsheet files that may be used for documenting test method specifications.
- Scanned images such as Case Report Forms.
- Electronic diagrams such as equipment layout diagrams maintained in a CAD program.
- Project files such as an MS Project Plan detailing test method development.

Within this section we shall consider the technical and procedural requirements for electronic records and electronic signatures in the FDA regulated environment as they relate to maintaining non-database electronic records.

The following technical requirements are relevant to non-database electronic records:

- Maintain a secure computer generated time-stamped audit trail to record date and time of operator entries and actions that create, modify or delete electronic records.
- Ensure that record changes shall not obscure previously entered data.
This requirement may be met by retaining previous document versions.
- Limit access to authorized qualified individuals held accountable by written policies.
Allow for varying levels of access (edit, view only) based on user ID.
- Generate accurate and complete copies of records in both human-readable and electronic form.
- Protect records to ensure their accurate and ready retrieval throughout the records retention period.
- If electronic records are transmitted across an open system (i.e. the Internet), ensure the record's authenticity, integrity and confidentiality from creation to receipt through the adoption of measures such as document encryption and digital signature standards.

The following additional technical requirements apply, if electronic signatures are executed to the non-database electronic records:

- Require a unique user ID and password, or biometric identification for a signature event. Require the periodic modification of user access passwords (password aging).
- For any signing event, record the signer's name, signing date and meaning of signature. This information should be displayed whenever the record is viewed on screen, or printed.
- A technical link shall be maintained between the electronic signature and the electronic record that can not be excised, copied or otherwise transferred.
- Detect repeated unauthorized access attempts, and notify the system administrator or security officer.

Part 11 also specifies procedural and administrative requirements. The focus of these requirements is to ensure that a system that maintains electronic records (such as a document management system) has been properly implemented within a controlled environment.

Relevant administrative and procedural requirements for electronic records include:

- Validation of any computerized system that maintains electronic records.
Computer System Validation is defined as follows:
Confirmation by examination and provision of objective evidence that computer system specifications conform to user needs and intended uses, and that all requirements can be consistently fulfilled.
- Adequate controls over the distribution, access and use of systems documentation, to include change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.
- Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training and experience to perform their assigned tasks.
- Actively manage user access to include periodic review of system access rights. User Ids should be unique to a specific individual, and not reassigned.
- If hand written signatures are affixed to printed versions of electronic records, provide a technological link between the electronic record and the physical signing. This is referred to as a hybrid system where the 'system' has an electronic and a paper component.

If the electronic records shall be signed electronically, the following additional procedural and administrative requirements apply:

- Each user that shall provide their electronic signature must acknowledge that their electronic signature is legally binding.
- The organization must notify the FDA of their intention to use electronic signatures to meet predicate rule signature requirements.

Hummingbird DM Meets 21 CFR Part 11 Technical Requirements for Electronic Records

Hummingbird DM gives an organization the ability to create, organize and share non-database electronic records in a secure document library. It provides a way to store documents so that they are accessible to the people who need them. And it prevents access by people who don't. A Hummingbird DM library has the flexibility to manage a wide variety of electronic record file types. Hummingbird DM also has the functional capability to meet, when properly configured, the technical requirements for maintenance of electronic records as defined within 21 CFR Part 11. Relevant functionality includes:

- Restrict electronic access to electronic records. Hummingbird DM may be configured so that electronic records are stored within a secure document server that may only be accessed via the Hummingbird DM application.
- Restrict user access to electronic records. Access to a Hummingbird DM library requires a valid User ID and password. The level of access to specific record maintained within a Hummingbird DM library may be specified at the user, group, document and folder level.
- Record information about electronic record. Hummingbird DM allows for information about electronic records to be maintained, such data would include, author, creation date, and edit date.
- Require that each modification to a document be retained as a distinct version. Hummingbird DM can be configured to force versioning, ensuring that each change to a document is recorded to an audit trail. The DM "Publish" feature ensures that the correct version is disseminated and prevents the deletion of a document version.
- Control dissemination of electronic records. While Hummingbird DM through its web interface provides wide access to electronic records, the product may be configured to restrict the dissemination of these records. The Hummingbird DM product can be configured to control the copying of electronic records. The product may also be configured to affix a restricted use watermark on printed versions of electronic records.

For a more detailed analysis of the requirements of 21 CFR Part 11, please refer to Appendix A.

Integrating *ApproveIt*⁺ Electronic Signature Software with Hummingbird DM Meets 21 CFR Part 11 Technical Requirements for Electronic Signature

Hummingbird has partnered with Silanis Technology to provide an electronic signature solution that complements Hummingbird DM. Silanis' *ApproveIt* Signature software allows for digital signatures to be embedded within the file format of leading general business applications such as Microsoft Word and Adobe Acrobat. The addition of this product allows for the electronic signing of electronic records maintained within a Hummingbird DM library.

This product when properly deployed meets the technical requirement of 21 CFR Part 11 for electronic signatures by providing the following technical capabilities:

- User ID and password are required to electronically sign a document. Silanis' security model meets Part 11 requirements for electronic signatures.
- At each signing event, the signer's name, signing date and meaning are recorded and inextricably linked to the signature. This information is included whenever the record is viewed on screen, or printed.
- Digital signature technology employed to ensure the integrity and authenticity of the signed electronic records even if that record is transmitted across a public network.
- Digital signature is embedded within the signed document's native file format. This approach ensures that a link is maintained between the electronic record and the electronic signature. This approach also allows for the seamless integration of e-signatures for files maintained within a Hummingbird DM document library.
- *ApproveIt's* administrator module detects unauthorized access attempts and generates system notification messages to alert the system administrator.

Hummingbird RM Complements Hummingbird DM to Facilitate Compliance through Good Electronic Records Management

Hummingbird RM transforms Hummingbird DM into a fully functional Records Management Application, thereby improving an organization's ability to exercise documented control over their electronic and physical records throughout the document life cycle. While Hummingbird RM is not required for Part 11 compliance, the proper employment of Hummingbird RM can facilitate Part 11 compliance through the automated definition and enforcement of Good Electronic Record Management (GERM) practices. FDA's draft "Guidance for Industry 21 CFR Part 11; Electronic Records; Electronic Signatures Maintenance of Electronic Records" emphasizes that an organization must employ procedures and controls to ensure the "protection of records to enable their accurate and ready retrieval throughout the record retention period" (21 CFR Part 11.10(c)).

Hummingbird RM functions are available from the DM client. Key functional enhancements provided by Hummingbird RM include:

- For each electronic record, records record management information such as review date, and retention period. These data are used to facilitate the record's periodic review and eventual destruction.
- Supplements the security features available in Hummingbird DM with functional security and term-level security. Hummingbird RM provides safeguards that an electronic record's meta data is not altered or lost.
- Definition and enforcement of retention and disposition policies (File Plans) for electronic records. This capability allows for a group of electronic records (such as case report forms) to follow the same review and retention policy.

Deploying Hummingbird Products to Comply with 21 CFR Part 11

Regulatory compliance of an installed electronic document management system requires not only that a tool be technically capable of meeting the rule, but also requires the tool's proper configuration and implementation within a controlled environment. Therefore, a document management system can not be "Part 11 Compliant," only "Part 11 Capable." Complete compliance can only be achieved through the proper implementation of a tool that has the functionality to meet 21 CFR Part 11's technical requirements.

Validation

Systems that maintain electronic records are subject to FDA requirements for validation. Validation encompasses the software, hardware, people and procedures. Validation can most simply be described as the thorough documentation of the system development life cycle, with a focus on developing objective evidence that the system meet its defined requirements. Generating and maintaining system design and test documentation shall present a significant challenge, but as far as the FDA is concerned, if it hasn't been documented, it hasn't been done.

Validation of a COTS (commercial off-the-shelf) application, such as Hummingbird DM and Hummingbird RM software, differs from the process used to validate internally developed custom applications. FDA's draft "Guidance for Industry 21 CFR Part 11; Electronic Records; Electronic Signatures Validation" provides the following guidelines for validating COTS application:

- Develop user requirements specification.
 - Requirements document should include Part 11 technical requirements.
 - Compare user requirements against the technical functionality of the document management system.
- Verify software's structural integrity.
 - Evaluate software for known limitations, software problems, and other end user experiences.
 - Evaluate supplier's software development activities to determine conformance to contemporary standards. (Vendor audit.)
- Functional Testing of Software.
 - Verify that program reliably meets end user requirements specification.
 - Testing should be limited to the program functions to be used.
 - If the end user cannot review supplier's development documentation, more extensive functional testing may be warranted.
- Document Implementation.
 - Document baseline configuration and any configuration changes post production.
 - Provide and document staff training. Ensure staff's qualifications are properly documented.
 - Develop and maintain "As Built" design documentation.
 - Identify the hardware and software components that comprise the system.

Validation is not a destination, but a journey; validation requirements must be integrated throughout the life cycle of the system from planning through retirement. In the remainder of this section, we shall provide some practical guidance regarding the deployment of Hummingbird products within the regulated environment.

Product Planning

The Hummingbird products are powerful and highly configurable tools for the management of electronic records. Successful deployment of such a tool within the regulated environment will require well documented and careful planning.

The first step is for the client to define their requirements for electronic records management. The User Requirements document should define the desired system functionality, incorporating both business requirements and Part 11 technical requirements. Each specific requirement should be uniquely numbered and written so as to be verifiable during testing.

The second step is to evaluate Hummingbird product functionality against the defined requirements. This evaluation should identify any requirements met through specific product configuration settings, while identifying requirements not met by the Hummingbird solution. Each unmet requirement should be evaluated for criticality and possible alternative approaches to meet the requirement.

The third step of the planning process is to document the system design thereby providing the technical blueprint defining the hardware and software that shall comprise the document management system. At a minimum, system design documentation shall include:

- **Hardware Diagram(s)** — depiction of each hardware platform that shall host a component of the deployed Hummingbird solution such as the document server, SQL database, application and index servers, and data backup devices. The diagram should depict the network linking the various hardware components and the system users.
- **COTS Software Listing** — this listing should define each version release of the software used within the Hummingbird system to include version information for all Hummingbird products/components, SQL database, and the integrated report writer. This listing should identify which deployment options shall be made available to clients. For example, it should specify if any custom software needs to be deployed to the Hummingbird DM client.
- **Custom Software Listing** — the Hummingbird products support significant customization of forms and reports via a form designed and API. Each customized item released into the production environment should be listed. To simplify ongoing maintenance, a brief description of each custom component's purpose should be provided.

Product Configuration

Proper product configuration is essential for regulatory compliance. Hummingbird DM, the core of Hummingbird's document management solution, is highly configurable with over 500 configuration settings. Many of these settings directly impact security and document versioning. A properly configured document management system can dramatically improve access to electronic records while ensuring the integrity of the electronic record. However, if system access is improperly controlled, the confidentiality and integrity of electronic records is subject to compromise.

Restrictive configuration settings should be set at the system level, where these settings will be inherited by each defined group. Less restrictive configuration settings may then be defined for an administrative group so that they are able to maintain the application. Care shall be required to restrict access to this administrative group to users with proper training and need for this access.

Configuration settings should be maintained by the Hummingbird DM System Administrator. They are accessible from the DM Admin Tab from the Hummingbird DM Webtop toolbar and from the Windows Library Maintenance utility. In the table below, key Hummingbird DM configuration settings are identified. The table does not include Hummingbird RM settings. Hummingbird RM settings, specified within ini files, are not essential to Part 11 compliance.

Within the table the Objective column defines a configuration issue essential to regulatory compliance. The Relevant Configuration Settings column identifies the specific configuration settings impacting that objective. The configuration screen where the configuration item is set is provided within brackets.

Objective	Relevant Configuration Settings
Prevent electronic records from being altered outside of Hummingbird DM control.	Secure Documents at Network Level [Features]
Ensure that user login is required each time a Hummingbird DM library is accessed.	Allow Auto Logon. [Defaults] Accept User Supplied Identification [Features] Supply Credentials Every Time. [Permissions]
Restrict access to system administration features to appropriate users.	Run DM Admin. [Utilities] Manage Library Parameters. [Utilities] Manager Users and Groups. [Utilities]
Prevent users from creating and deleting folders within a regulated Hummingbird DM library.	Can Create/Remove Public Folders. [Permissions] Can Create Folders. [Permissions]
Restrict user access to the current effective version.	Allow Document Checkout.[Defaults] Allow Copy of In Use Documents. [Defaults] Allow Publish Version. [Versions] Allow Unpublish Version. [Versions] Multiple Published Versions. [Versions]
Prevent approved documents from being modified or deleted.	Allow Users to Delete Documents. [Defaults] Allow Users to Delete Content. [Defaults] Allow Users to Delete Versions. [Defaults] Allow Make Read Only. [Versions] Allow Make Version Read Only. [Versions] Allow Remove of Read Only. [Versions] Allow Remove of Version Read Only. [Versions] Make New Version from Any Version. [Versions]
Prevent an approved document version from being overwritten.	Edit Previous Versions. [Versions] Allow Overwrite of Simultaneous Edits. [Attaché]
Prevent proliferation of uncontrolled copies of electronic records.	Disable Native Open/Save. [Defaults] Shadow Files to Local Drive. [Attaché] Shadow Secured Documents. [Attaché] Allow Edit of Shadowed Documents. [Attaché]
Control access to document information data.	Allow Mass Updates to Profiles. [Defaults] Profile Level Security. [Defaults] Visit Author Requested Edit. [Versions] Visit Entered By. [Versions]

The proper Hummingbird configuration settings must be documented at baseline. This can most simply be achieved by capturing screen prints of the system configuration setting screens and print-outs of any relevant ini files.

Other Implementation Considerations

Implementing Hummingbird DM involves creating the environment defined within the product planning and configuration phases while ensuring the security of the system. Additional requirements are defined below.

SQL Database Security

While proper Hummingbird DM configuration can ensure security of the application and electronic records within the document server, the security of the SQL database that contains document information also must be ensured through the proper administration of the SQL database. The Hummingbird DM installation plan should ensure proper database security by verifying:

- Default SQL database passwords have been modified.
- Database user accounts should be restricted to the one required system account and DBA accounts.

Written Procedures

To provide evidence that the document management system is maintained and used within a “controlled environment,” written procedures should be developed that define the responsibilities and the process for system management and maintenance. This written guidance should be completed prior to system testing because some user requirements may only be met through defined procedures. At a minimum, written procedures should be developed to cover the following issues:

- ***Hummingbird System Administration*** — this procedure would define responsibilities for the ongoing administration of the Hummingbird application to include:
 - Process for adding and removing users, and changing access rights.
 - Definition of ongoing maintenance tasks.
 - Detail the requirements to verify any change made to the system via a change control/configuration management process.
 - Specify technique to be employed to place a restriction on the use of electronic records printed from the Hummingbird interface.
- ***General IT Support for the Hummingbird applications*** — this procedure would define the process for backup of the Hummingbird DM Database, Document Server and Application Server. It should also identify responsibilities and action plans for disaster recovery and business continuity planning.
- ***Client Specific Hummingbird Users Guide*** — while Hummingbird provides extensive user documentation, the method in which the application shall be employed will likely vary for each organization. A procedure should define common conventions to be used, to include defining the concept of working draft and approved document. This document should also define the process for linking physical signings to electronic records.

System Testing

The purpose of system testing is to provide objective evidence of the software's proper implementation, and that the product as implemented meets its defined requirements. For a COTS package such as Hummingbird DM this requirement can most simply be met through the installation and system testing approach as briefly defined below.

Installation Plan and Report

The objective of the installation plan is to identify the configurable components subject to verification and the documentation that shall be referenced to verify their proper implementation. The installation plan then identifies the process to be followed to verify that the Hummingbird products have been installed and configured in accordance with the system design documentation.

The installation report documents the results of the installation plan's execution, providing objective evidence of the proper implementation of the Hummingbird products. Attached to the installation report should be screen prints of key Hummingbird configuration screens and ini files.

Develop and Execute Test Scripts

After the completion of the installation report, the system testing process shall verify that the Hummingbird system as implemented meets the defined user requirements. At a minimum a system test plan and one or more test scripts shall be developed. The test plan defines all the test scripts to be executed, and provides a cross reference matrix that depicts how the execution of the test scripts shall verify that each user requirements was met. Test scripts should be developed to capture objective evidence that each user requirement was met, and include challenge tests to verify reliability in the face of unexpected inputs.

Each test script should contain the following information prior to its execution:

- **Test Instructions** — provide specific instructions on how to perform the test and document its results. The test instructions should provide enough detail so that testing is reproducible.
- **Reference to user requirement(s) being tested** — identify specific user requirements to be verified within the test script.
- **Expected Result** — specify the anticipated result of the test script.

During test execution the following additional information should be recorded:

- **Actual Result** — record the tester's observations or reference objective evidence of test results such as screen prints or report output.
- **Pass/Fail Evaluation** — the tester shall compare the actual results observed against the expected results. When these results are consistent the test is evaluated as Pass. If the test cannot be executed as written or the actual results differ from the expected results the test should be evaluated as Fail.
- **Tester Initials and Date** — each pass/fail designation should be attributable to a specific date and tester.

This testing provides the foundation of the validation package, and should be formalized as follows:

- Approval of Test Plan and pre-approval of test scripts prior to execution as evidenced by dated signatures.
- Collection of objective evidence referenced in Actual Result column so that reviewer may reach same conclusion as tester.
- Review of each test script by a competent technical reviewer. The tester and reviewer should sign and date each test script.
- Approval of executed test scripts as evidenced by dated signatures.

Ongoing Operation and Maintenance

Following successful system testing, the Hummingbird system may be placed into production. Controls over the use and any changes to the application shall be required as long as the system maintains FDA regulated electronic records. Key requirements during maintenance include:

Training Records and Qualifications

Evidence of proper user and administrator training should be maintained for validated systems. Successful completion of training should be a pre-requisite for gaining system access. The training program must remain effective to ensure that new users are trained in system use, and existing users are provided refresher training as the Hummingbird applications evolve over time.

Part 11 also requires that technical and administrative staff that maintain the Hummingbird system be qualified for their positions. This requirement can be met by satisfying the following conditions:

- Each staff member is clearly assigned a specific position.
- A position description is maintained for each position, to include the qualifications required of the position.
- A training record is maintained for each staff member that documents that the staff member meets the qualification requirements of their assigned position.

Configuration Management/Change Control

Any change to the Hummingbird system's hardware or software components shall be documented and tested prior to being placed into production. The process for managing the configuration process should be documented within a written change control procedure.

Examples of system changes subject to change control include:

- Upgrade or modification to system hardware.
- Upgrade or revision to existing Hummingbird product installation.
- Custom modification to Hummingbird products such as the modification of a screen template.

The change control process should ensure that the following actions occur to properly document and verify the change:

- Proposed change subjected to a documented review and approval process prior to implementation.
- Changes are verified prior to being placed into production, and evidence of the verification is recorded within a change control record.
- Any configuration change subject to defined configuration management review process.
- System design documentation is updated to reflect the change. It is essential that "As Built" design documentation is maintained while the Hummingbird system remains in production.

Conclusion

Hummingbird DM, when properly configured, satisfies 21 CFR Part 11 technical requirements for the management of non-database electronic records to include access control and auditing. Hummingbird DM libraries can be developed to contain electronic records subject to 21 CFR Part 11 that are created and modified by general business applications to include SOPs, spreadsheet files, drawings and project plans.

Hummingbird DM provides an environment for maintaining non-database electronic records. With the addition of Hummingbird RM and Silanis' *ApproveIt* software, Hummingbird DM may be extended into a comprehensive document management system:

- Silanis *ApproveIt* electronic signature software integrates with Hummingbird DM to allow for the affixing of electronic signatures to electronic records.
- Hummingbird RM extends Hummingbird DM to provide comprehensive records management capabilities for both physical and electronic records.

Any system that is used to maintain electronic records, to include document management systems, is subject to FDA requires for computer system validation. Validated systems must be well documented to include User Requirements Definition, "As Built" System Design documentation, evidence of system testing and configuration management/change control records.

During system implementation and system use the emphasis must be on document control, not uncontrolled document dissemination. The practical standard for evaluation of automated document management system is its paper based predecessor. As stated by the FDA within 21 CFR Part 11 electronic records "...should be trustworthy, reliable, and generally equivalent to paper records and hand written signatures executed on paper." Hummingbird DM and supporting products provides firms with the flexibility and functionality to meet this expectation for their non-database electronic records.

Appendix A

Within this appendix the ability for the Hummingbird DM, Hummingbird RM and *ApproveIt* products to meet the technical requirements of Part 11 is evaluated. This evaluation covers the relevant Part 11 requirements, and provides an approach towards meeting those requirements. Many of the requirements can only be met through administrative action or through the adoption of written procedures. Compliance with those aspects of the regulation are the responsibility of the firm implementing the software.

Subpart B — Electronic Records

Section 11.10 Controls for Closed Systems

Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

	21 CFR part 11 requirement	Requirement Type	How Requirement is Met
1	(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Administrative	Guidance available within main document and from FDA Draft Guidance “Electronic Records; Electronic Signatures: Validation.”
2	(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency.	Technical	Hummingbird DM supports viewing and printing of files in native formats to ensure that the record when viewed to screen, printed or copied is an accurate and complete representation of the record. Access to this capability is configurable at the document, folder, user and group levels.
3	(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Technical	Proper configuration of Hummingbird DM protects electronic records from unauthorized external access, and allows for controlled access via Hummingbird DM. Hummingbird RM facilitates the definition and enforcement of a comprehensive records management and retention policy.
4	(d) Limiting system access to authorized individuals.	Technical	Hummingbird DM security requires a valid user ID and password to gain access to electronic records. Hummingbird DM security can be synchronized with network security. Hummingbird RM adds additional security to protect access to corporate records.

	21 CFR part 11 requirement	Requirement Type	How Requirement is Met
5	(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	Technical	Hummingbird DM can be configured to ensure that each approved document is retained throughout the document's retention period, and that each version is linked to an author, the version's time and date, and the operator who updated the record. Through retention of all past approved versions, previous approved document data shall not be obscured. Hummingbird DM also includes an audit trail that records all actions performed on a document, the time of the action, and the identity of the person performing the action.
6	(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Technical	The Hummingbird DM WorkFlow™ module is an optional component of the Hummingbird DM product suite. This module enables the definition and enforcement of document draft, review and approval processes.
7	(g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	Technical	Hummingbird DM allows for the level of access rights to specific electronic records or group of records to be defined at the user, group, document or folder levels. The <i>ApproveIt</i> electronic signature application also requires a user to have a valid user ID and password.
8	(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Technical	The Hummingbird DM product suite includes the optional Hummingbird Imaging component. Verification of device inputs (scanners) to the imaging process would be part of the system validation effort.
9	(i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	Administrative	Hummingbird provides a variety of Hummingbird DM product training courses for users through system administrators. The use of the Hummingbird DM product suite is well documented through an extensive set of user manuals. These user manuals can provide the basis for an internal training program.
10	(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	Procedural	A validated application requires that the application's use and maintenance be defined within a written procedure. This requirement can be met through a written procedure and its enforcement.
11	(k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	Procedural	(1) As part of the validation process, system documentation defining the hardware and software components of the Hummingbird DM product suite shall be developed. (2) Storage of this documentation within a Hummingbird DM product library and treatment of the system documentation as an electronic record would satisfy this requirement.

Section 11.20 Controls for Open Systems

Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in § 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

Requirement Analysis — An open system is defined by the FDA as “an environment in which system access is not controlled by persons responsible for the content of electronic records that are on the system.” Perhaps the most pertinent example of an Open System is Internet Mail where the message and its contents are outside of the control of the originating organization. Hummingbird DM has the ability to support this requirement through encryption capabilities and the use of digital signature technology within the *ApproveIt* electronic signing capability.

Section 11.50 Electronic Signature Manifestations

	21 CFR part 11 requirement	Requirement Type	How Requirement is Met
12	(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: (1) The printed name of the signer; (2) The date and time when the signature was executed; and (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	Technical	Hummingbird DM has partnered with <i>ApproveIt</i> for providing electronic signature capabilities for signing documents maintained within a Hummingbird DM library. The <i>ApproveIt</i> application records the signer’s ID, date and time of signing and allows for the recording of the meaning of the signing.
13	(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency.	Technical	<i>ApproveIt</i> embeds the digital signature within the document. Any workstation with <i>ApproveIt</i> installed that opens and prints the record shall be able to view and print the signature. If <i>ApproveIt</i> is not installed then an image is presented on screen and in print that lets the user know the document has been signed.

Section 11.70 Signature/Record Linking

	21 CFR part 11 requirement	Requirement Type	How Requirement is Met
14	Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.	Technical and Procedural	For electronic signatures affixed by <i>ApproveIt</i> , the digital signature is embedded in the native format of the electronic record. This approach ensures strong linking. For linking handwritten signatures executed to electronic records shall require both a written process as well as the ability to provide a technical link to the record. Hummingbird DM does provide a unique reference number for each version of a document.

Subpart C — Electronic Signatures

Section 11.100 General Requirements

	21 CFR part 11 requirement	Requirement Type	How Requirement is Met
15	(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	Administrative	Hummingbird DM has partnered with <i>ApproveIt</i> for providing electronic signature capabilities for signing documents maintained within a Hummingbird DM library. The <i>ApproveIt</i> application records the signer's ID, date and time of signing and allows for the recording of the meaning of the signing.
16	(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.	Administrative	The <i>ApproveIt</i> signature process includes digitizing each signer's handwritten signature, providing the user with a clear connection between their handwritten and electronic signatures. The process for authorizing and enabling electronic signature authority for a staff member should be documented within a written procedure.
17	(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system are intended to be the legally binding equivalent of traditional handwritten signatures.	Administrative	Should be part of the electronic signature implementation process.

Section 11.200 Electronic Signature Components and Controls

	21 CFR part 11 requirement	Requirement Type	How Requirement is Met
18	(a) Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password. (i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. (ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components. (2) Be used only by their genuine owners; and (3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.	Technical and Administrative	<i>ApproveIt</i> does require two distinct identifications: user ID and password. <i>ApproveIt</i> and Hummingbird DM are not tightly integrated. <i>ApproveIt</i> does not have a concept of a signature session. The solution is simply to require that the signer enter a User ID and password for each electronic signature execution. Items 2 and 3 require that appropriate administrative procedures be in place to ensure that users are trained in maintaining the integrity of their password security by not sharing it with others or writing their password down in a public location.
19	(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	Technical	<i>ApproveIt</i> does not currently support Biometric input in lieu of User ID/Password authentication.

Section 11.300 Controls for Identification Codes/Passwords

	21 CFR part 11 requirement	Requirement Type	How Requirement is Met
20	(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	Technical	<i>ApproveIt</i> requires that a user ID be unique.
21	(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	Technical and Procedural	This requirement is best meant through a combination of functional capability and written procedural guidance. <i>ApproveIt</i> may be configured to require that users change their password on a quarterly or semi-annual basis. This should be combined with a defined process where access is reviewed on an annual basis.
22	(c) Following loss management procedures to electronically de-authorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.	Procedural	Not relevant to Hummingbird DM — <i>ApproveIt</i> electronic signature approach.
23	(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.	Technical	No inherent notification capability, but <i>ApproveIt</i> and Hummingbird DM can detect and record failed access attempts. The product could then be customized to generate an e-mail notification using a tool such as Send Mail.
24	(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.	Procedural	Not relevant to Hummingbird DM — <i>Approve It</i> electronic signature approach.

Corporate Headquarters

1 Sparks Avenue

Toronto, Ontario M2H 2W1

Canada

Toll Free Canada/USA:

+1 877 FLY HUMM (359 4866)

Tel: +1 416 496 2200

Fax: +1 416 496 2207

E-mail: getinfo@hummingbird.com

North American Sales Offices

Boston • Chicago • Dallas • Los Angeles

Mountain View • New York • Ottawa

Raleigh • Toronto • Washington DC

International Sales Offices

Amsterdam • Berlin • Brussels • Frankfurt • Geneva

Hong Kong • London • Milan • Munich • Paris • Rome

Seoul • Singapore • Stockholm • Sydney • Tokyo

Wokingham • Zurich

For more information, visit

www.hummingbird.com/wp/fda

Copyright © 2003, Hummingbird Ltd.
All rights reserved.

® ™ — Trademarks and logos are the
intellectual property of Hummingbird Ltd.

† — Approvelt is a trademark of Silanis Technology.
All other company and product names are
trademarks of their respective owners.

WP-04-00-EN-0023.04/03
Printed in Canada.

