

*How iMedRIS Addresses the Requirements of*

# **FDA 21 CFR Part 11**

*in Closed Systems*

## **iMedRIS Data Corp.**

446 Missouri Court  
Redlands, CA 92373  
(909) 798-9100  
(909) 798-9102 FAX  
[www.iMedRIS.com](http://www.iMedRIS.com)

## Contents

Title 21 Code of Federal Regulations (21 CFR Part 11) Electronic Records; Electronic Signatures came into effect on August 20, 1997 and sets forth criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper. People using electronic signatures must certify to the agency that the electronic signature in their system is intended to be the legally binding equivalent of traditional handwritten signatures.

## Subpart A – General Provisions

### 11.1 Scope

*(a) The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.*

*(b) This part applies to records in electronic form that are created, modified, maintained, archive, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part 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 agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.*

*(c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically accepted by regulation(s) effective on or after August 20, 1997.*

*(d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with Sec. 11.2, unless paper records are specifically required.*

*(e) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.*

### 11.2 Implementation

*(a) For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.*

*(b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that:*

*(1) The requirements of this part are met; and*

*(2) The document or parts of a document to be submitted have been identified in public docket No. 92S-0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.*

### **11.3 Definitions**

*(a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.*

*(b) The following definitions of terms also apply to this part:*

*(1) Act means the Federal Food, Drug, and Cosmetic Act (secs.201-903 (21 U.S.C. 321-*

*393)). (2) Agency means the Food and Drug Administration.*

*(3) Biometrics means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.*

*(4) Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.*

*(5) Digital signature means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.*

*(6) Electronic record means 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.*

*(7) Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.*

*(8) Handwritten signature means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.*

*(9) Open system means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system*

## Subpart B – Electronic Records

### 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:*

### System Validation

*11.10(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.*

### iMedRIS Statement

System validation is performed using a risk-based approach to the software. Risk is determined considering elements such as: subject safety, erroneous data, and software security. Essential components of the software have been tested for accuracy, reliability, and functionality using specific test cases.

The FDA states in section 5.1 of their "Draft Guidance for Industry, 21 CFR Part 11; Electronic Records; Electronic Signatures Validation" document, *"Regardless of whether the computer system is developed in-house, developed by a contractor, or purchased off-the-shelf, establishing end user (i.e., a person regulated by the FDA) requirements is extremely important for computer system validation. Without first establishing end user needs and intended uses, we believe it is virtually impossible to confirm that the system can consistently meet them."* In section 5.2, the FDA further states, *"We consider thorough documentation to be extremely important to the success of our validation efforts. Validation documentation should include a validation plan, validation procedures, and a validation report, and should identify who in management is responsible for approval of the plan, the procedures and the report."*

### Validation Logs

Validation logs are kept in a concurrent version system (CVS); with each subsequent version not replacing the old version. A hardcopy of the current working version is kept by authorized iMedRIS personnel.

Test cases validate that:

- Functions on a screen work correctly
- Added records function as intended
- Input data is accurate when viewed
- User access is limited to role
- Electronic signatures cannot be copied, forged, or illegally accessed.

Test cases are authored by an iMedRIS staff member, who has been trained on the intended process of the software. The test case is run by another iMedRIS staff member, and finally reviewed by an iMedRIS project manager. See Alternative Validation Procedures for failed test cases.

### **Alternative Validation Procedures**

When a test case does not pass, a request is issued to a software engineer to correct the issue that failed the test case. When the issue is resolved, the same test will be run, but it will be attached to the original documentation and will not replace the original test case.

For each new release of iRIS™, only components of the software that have been modified, added or would be affected by a modified or added component are validated. Each new version of validation does not replace old versions in the CVS.

*11.10(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. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.*

All records and audit trails recorded in iRIS™ are printable in both human readable and electronic form suitable for inspection, review and copying by the agency if needed.

### **Data Availability**

*11.10(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.*

### **iMedRIS Statement**

The issue of data accuracy is dependent upon the client. It is their responsibility to ensure accurate data is entered into iRIS™.

The issue of data availability is more than adequately addressed in iRIS™ in the following ways:

1. Files are located in user-specific directories on the local drive or network drive and can, therefore, be easily retrieved.
2. The system audit trail includes a log of all records that have been created on the system. The system audit trail (master) resides on the server computer. The system audit trail is a mirror copy of the master database table which contains all modification transactions to a record.
3. This audit table can be queried to show all historical user modifications to a single record.

### **Validation**

1. Check user directories for specific files.
2. Create record in iRIS™:
  - a. Record created: User training record for user cackerman (see screenshot below)
  - b. Date created: 03/08/2010

User Administration - Training record list for Ackerman, Catherine D

**\*User\_ID:** cackerman      **Name:** Catherine D Ackerman  
**Job Title:** Quality Assurance Engineer      **Status:** Active      **Login Enabled:** Yes  
**Degree:**      **Contact Information:**  
**Employee ID:**      **Email Address:** catherineAckerman@gmail.com  
**Social Security Number:**      **Primary Number:** 909-555-1234  
**Specialty:**      **Cell Number:**  
**Affiliations:**      **Pager Number:**  
**Other Affiliation:**      **Fax Number:**      **Mailing Address**  
**Location:** 123 Main Street  
 Katy, TX 73223

<input type="checkbox"/>	Edit/View	Training Group	Courses (Course Date - Expiration)	Status	Override
(default)		IRB	Training Course - ( 04/03/2008 - 04/16/2010) Training Course - ( 07/31/2007 - 07/30/2009) Training Course - ( 04/09/2008 - 04/09/2009) Training Course - ( 07/31/2007 - 07/30/2008)	Active	No
(default)		IACUC	Training Course - ( 07/20/2009 - 07/20/2010)	Active	No
<input type="checkbox"/>		Vaccination		Expired	No
		Mathematics Major	Discrete - ( 03/08/2010 - 03/08/2011)	Expired	No

c. Check audit trail for created form type (see screenshots below\*)

System Administration - Data Audit

User ID:         
 Begin Date: 03/02/2010  
 End Date: 03/10/2010  
 Tables:
 

- Contract Account
- Contract Account Payment
- Contract Agreement Review
- Contract Agreement
- Contract Disclosure
- Contract Document Archive
- Compliance Non-Study Document
- Compliance Study Document

3 result(s) found... 1 - 3

Details	Table Name	Modified By	Date Modified	Action
	A_USER_TRAINING	mwhitehead	March 08, 2010 11:23:45 AM	I
	A_USER_TRAINING	mwhitehead	March 08, 2010 11:24:23 AM	U
	A_USER_TRAINING	ADMIN	March 09, 2010 03:30:02 AM	U

Column	Value
PK_INDEX	101
USER_TRAINING_ID	223
USER_ID	79
STATUS	Active
TRAINING_GROUP_ID	3
OVERRIDE_FLAG	No
ID_CREATED	164
DATE_CREATED	2010-03-08 11:23:45.547
ID_MODIFIED	164
DATE_MODIFIED	2010-03-08 11:23:45.547
ACTION	I

(Screenshot of record details. User cackerman has USER\_ID of 79)

3. Create and submit a new study (see the screenshot below)

- a. Study number: Test 123
- b. Time Submitted: 03/09/2010

Open	Pending - Submitted for Initial Review		Whitehead, Matt Anthony	Test 123	Copy
------	--	--	-------------------------	----------	------

c. Check audit trail for created study (see the screenshot on the following page\*)

System Administration - Data Audit

User ID:  Search

Begin Date: 03/09/2010

End Date: 03/10/2010

Tables:

- Contract Account
- Contract Account Payment
- Contract Agreement Review
- Contract Agreement
- Contract Disclosure
- Contract Document Archive
- Compliance Non-Study Document
- Compliance Study Document

60 result(s) found... 51 - 60

Details	Table Name	Modified By	Date Modified	Action
	A_STUDY_SUBMISSION	mwhitehead	March 09, 2010 10:11:10 AM	U
	A_STUDY_SUBMISSION	mwhitehead	March 09, 2010 02:00:39 PM	I

\* In the audit trail I = Insert (creation of a record), U = Update (edit of a record) and D = Delete (deletion of a record)

Column	Value
PK_INDEX	7610
SUBMISSION_ID	963
MASTER_SUBMISSION_ID	963
PARENT_SUBMISSION_ID	null
RESPONSE_SUBMISSION_ID	null
CLONED_FROM_SUBMISSION_ID	null
SYSTEM_STUDY_ID	574
STUDY_ALIAS	Test 123
STUDY_TITLE	Test 123
SUBMISSION_DATE	2010-03-09 14:01:02.83
PREVIOUS_SUBMISSION_TYPE	0
SUBMISSION_TYPE	12
DATA_ID	6442
COPY_DATA_ID	null
SUBMISSION_SENT	Yes
HAS_SIGNOFF	Yes
SIGNOFF_COMPLETE	Yes
KSP_VALIDATION	Yes
KSP_COMPLETE	Yes
DEPARTMENT_ID	null
SUBMISSION_FORM_NAME	Initial Review Submission Form
CREATED BY	-1

## Limiting Access

*11.10(d) Limiting system access to authorized individuals.*

### **iMedRIS Statement**

User access is limited to certain departments and roles. User capabilities depend upon these roles.

### **Validation**

#### ***Study Management Access***

1. Assign user access to the study:
  - a. Roles/users:
    - i. irispi, Principal Investigator
    - ii. fttest, Co-Investigator
    - iii. mtest, Study Coordinator
  - b. Study Number: TS 002
2. User has access?
  - a. irispi has access
  - b. fttest has access
  - c. mtest has access
3. User not assigned has access?
  - a. User jsmith cannot find study
  - b. User gtest cannot find study
4. Add user after study has been submitted to the review board?
  - a. Cannot add KSP to study after it has been submitted.

#### ***Review Board Access***

1. What review board roles can access the study?
  - a. Administrative role
  - b. Coordinator
  - c. All other review board member roles have a limited access to the study.
2. What roles can review the study?
  - a. Administrative role and Coordinator have ability to assign designated reviewers to the study.
3. What roles have voting rights on the study?
  - a. When a user is specified a role in the review board, the System Administrator must specify if the user will have voting rights.
4. Can the submission be altered by a review board member?
  - a. Any submission made is read-only
5. Can review board members add KSP?
  - a. Any review board member has the ability to add a KSP to a study that has been submitted.

#### ***Administrative Access***

1. User roles that have access to the study, but are not associated to the study:
  - a. System Administrator
  - b. Site Assistant Department Administrator, if associated with the same department

## Audit Trails

11.10(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.

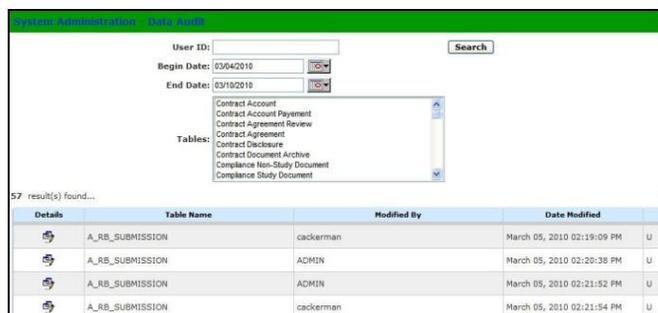
### iMedRIS Statement

iRIS™ contains an Audit Trail for all critical tables (changes to the system settings and data entry). Tables are considered to be critical on a risk based assessment by iMedRIS personnel. Each entry is time and date stamped. The audit trail records modifications capturing data column changes with extra information which includes the record creation date and user ID at creation time. The user ID and date modified are supplied in the audit trail so it is easy to determine exactly who made the changes.

This ensures that our audit trail identifies who performed the action within the software.

### Validation

1. Each database transaction is audited which captures every INSERT, UPDATE, and DELETE to a mirror audit table.



Details	Table Name	Modified By	Date Modified	
	A_RB_SUBMISSION	cackerman	March 05, 2010 02:19:09 PM	U
	A_RB_SUBMISSION	ADMIN	March 05, 2010 02:20:38 PM	U
	A_RB_SUBMISSION	ADMIN	March 05, 2010 02:21:52 PM	U
	A_RB_SUBMISSION	cackerman	March 05, 2010 02:21:54 PM	U

2. Each primary transaction is tested to verify it is structured correctly and further tested by stepping the programming through the code using a debugger.
  - a. If the application logic involves dependent transactions, the transactions are placed in try catch structure (used to test a block of code for errors) with auto commit turned off (changes are not automatically accepted).
  - b. If no error occurs then the transaction is committed. Otherwise, the transaction is roll backed and no partial data is committed.

## Sequencing, Authority, and Device Checks

11.10(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

### iMedRIS Statement

iRIS™ application logic is structured in such a way which allows data entry when edit mode is permitted. When the record is complete or under review the record becomes read-only. This process ensures that only the appropriate user(s), based on a user-role, can modify or view a record through its life cycle.

## Validation

1. Based on the hard coded study statuses
  - a. Study Management access is allowed for all hard coded statuses
2. Based on System Administration configurable status
  - a. Study Management access is allowed depending upon configuration
3. Based upon Submission
  - a. During workflow routing, Review Board access is allowed

11.10(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.

## iMedRIS Statement

Only authorized users can access the iRIS™ software through a user ID and encrypted password validation process and electronically sign a record or perform the operation at hand. Records can only be altered by authorized users.

## Validation

1. Accounts are granted by the System Administrator
  - a. System Administrator assigns user name and password
2. Access is restricted based upon user role (see 11.10(d))
3. All electronic signatures require
  - a. User ID
  - b. User password
4. System checks validate that the user ID and password match the logged in user as well as if the user is the designated signer.
  - a. If user is not required to signoff, the user can still see the signoff page, but page is read-only (see screenshot on the following page)

The screenshot displays the 'Submission Signoff Sheet' interface. At the top, it shows the user is logged in as 'Administrator' from the 'CA-GH - Cardiology' department. The navigation path is 'Home > my studies > study mgmt. > track submission'. The main content area shows the 'Study Title' and 'Submission Form(s)'. Below this, there is a section for the Principal Investigator to approve or deny the submission. A note states that an electronic signature is required. The 'Investigator Assurance' section contains a list of responsibilities for the investigator, such as ensuring the research meets scientific and ethical criteria, complying with regulatory requirements, maintaining accurate records, and participating in the open publication of results. A 'View Other Comments' link is located at the bottom of the form.

The user, Administrator, is associated to the study, but is not required to sign off on the submission. Administrator can view the sign off page, but it is read-only.

*11.10(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.*

### **iMedRIS Statement**

Users can login from any computer with Internet access using their unique user ID and password. Users are then validated and allowed access based on their privileges set with in the software.

### **Validation**

1. Depending on the actual system, iRIS™ is accessible from any computer that meets system requirements and has network access to the iRIS™ Application server.
2. Access is restricted based upon user role (see 11.10(d))

## **Training**

*11.10(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.*

### **iMedRIS Statement**

It is the responsibility of the client to ensure that individuals have the education, training, and experience to perform their assigned tasks. iMedRIS Data Corporation offers user training during client setup and configuration as well as other educational opportunities after software implementation. The training is documented and performed by qualified service personnel.

### **Validation**

1. Initially, training is set up within the contract
2. Clients will request training as needed

## **Written Policies**

*11.10(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.*

### **iMedRIS Statement**

iRIS™ gives the client the ability to establish their own policies and assurances for electronic signatures. The client creates and implements these policies and assurances into the system. Adherence to these policies and assurances are solely the responsibility of the client. It is the responsibility of iMedRIS to inform the client of this feature.

### **Validation**

1. Client creates policies and/or assurances
2. Policies/assurances are implemented into the signoff page
3. By signing, user agrees to the written policy and/or assurance

## Revision Controls

*11.10(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.*

### **iMedRIS Statement**

All documentation for the iRIS™ application is subject to a validation process. Separate manuals are provided for each module purchased. Administrative documentation related to system security, user accounts and other sensitive functions are handled separately and are only available to assigned personnel. The assigned personnel are the responsibility of the client to define. (i.e. the Software Administration functionality and role)

Each time the iRIS™ system is updated, a complete listing of what was changed, problems corrected, or improvements added is provided to the client in Release Notes.

### **Validation**

1. Assigned iMedRIS personnel are responsible for creating and updating documentation.
2. All documentation is stored in a concurrent version system (CVS).
  - a. Allows only one copy of a document to be checked out for modifications at a time
  - b. Allows version tracking
  - c. Allows history comparison
3. Clients are supplied with documentation on an as-needs basis at an iMedRIS personnel's discretion.
4. Release notes are distributed to each client before or upon the release.

## Data Security in Open Systems

*11.30 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.*

### **iMedRIS Statement**

The iRIS™ application is not considered an Open system.

### **Validation**

According to 11.3 of this document:

*(4) Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.*

*(9) Open system means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system*

## Signature Manifestations

### 11.50 Signature Manifestations

(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.

### iMedRIS Statement

iRIS™ addresses paragraph (a) in the following ways.

- (1) The user's full name is retrieved from the personal contact demographic record for the logged-in user which will be displayed on any form or document after a signature is applied.
- (2) A date and time stamp is applied once the signature has been validated.
- (3) The “meaning” is associated with the type of document the user is electronically signing and is maintained for visual display whenever the signature is viewed. The signature can contain the ID of the user entering data. Each time a data point is changed, the timestamps are included in the iRIS™ audit logs which are captured on the data server database.

### Validation

At any time, the signoff page can be viewed to see the name of the user who applied the signature. See screenshot below.

The screenshot displays the 'Submission Signoff Sheet' interface. At the top, it identifies the user as Nathan Mossman from the Cardiology department. The submission is for 'Rick Study'. Below this, there is a link to review documents and a question asking for approval or denial. A section titled 'Investigator Assurance' contains a list of responsibilities for the investigator, such as meeting scientific and ethical criteria, complying with regulations, and participating in open publication of results.

(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).

## iMedRIS Statement

All human readable forms of the electronic record contain the decrypted electronic signature(s) as well as the associated information.

## Validation

Any time the electronic signature is viewed, it is in readable format.

The screenshot shows the iMedRIS Submission Signoff Sheet interface. At the top, there is a header with the iMedRIS logo and navigation links for Home, Logout, and Help. The user's account information is displayed as Principal A. Investigator, MD, Department: CA-GH - Cardiology, and Navigation: Home > study mgmt. The main content area is titled "Submission Signoff Sheet" and includes a "Back" button and a "Save Signoff" button. The "Study Title" is "An Exploratory Pharmacogenomic Study of Erbitux Mono Therapy in Patients with Metastatic Colorectal Carcinoma". Below this, there is a "Submission Form(s)" section with a link to "Click here to review the submission documents". The user is identified as "Principal A. Investigator, MD" and is asked to "Approve or Deny this submission?". There are radio buttons for "Approve" (selected) and "Deny". A link to "Click here to add comments." is also present. At the bottom, there is a login section with "User ID: irispi" and a password field. A "View Other Comments:" link is located at the very bottom of the form.

Signature is viewed and is readable.

## Signature/Record Linking

### 11.70 Signature/Record Linking

*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.*

## iMedRIS Statement

The electronic signature(s) are embedded in the electronic record and cannot be excised, copied, or otherwise transferred by ordinary means. A signature cannot be used by any other person, as long as the user's organization maintains proper security control of identification codes and passwords.

## Validation

1. When an electronic signature is applied the verification process places an acknowledgement in the database, including the date and time the signature is applied.
2. Forms that can be signed off on can be copied but if the form that is being copied contains a signature, the signature placeholder is zeroed out (deleted) indicating that the form is not signed.

## Electronic Signatures

*11.100(a) Each electronic signature shall be unique to one individual and shall not be re-used by or re-assigned to anyone else.*

11.100(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.

### iMedRIS Statement

Whenever the iRIS™ system administrator creates a new user account, the iRIS™ software validates each unique user ID and ensures that the user ID and password are not a duplicate in the system. The password is also encrypted in the database for additional security. In addition, password changes are required based on a configuration setting by the software administrator.

### Validation

1. The system.enforce\_strong\_password system property enforces the strong password (which must contain the items listed in the description of the screen shot below) if the property is set to "Yes".

system.enforce_strong_password	<input type="radio"/> Yes <input checked="" type="radio"/> No
<i>Description:</i> Passwords must consist of 3 characters from the following four sets: A-Z, a-z, 0-9, {}[],.<>;:?"/ \`~!@#\$\$%^&*()_+=. Also, system.min_password_length, will be checked upon password edit or creation.	

2. The system.min\_password\_length property requires the minimum amount specified in the text box to be used in the password.

system.min_password_length	<input type="text" value="5"/> <input type="checkbox"/> Check to encrypt permanently
<i>Description:</i> Set the minimum amount of characters in the password.	

3. The system.password\_alpha\_numeric property requires the use of letters and numbers in the password, if set to "Yes".

system.password_alpha_numeric	<input checked="" type="radio"/> Yes <input type="radio"/> No
<i>Description:</i> Enter ""Yes"" to use numbers and letters in the password, enter ""No"" not to enforce alpha numeric passwords.	

4. The above said system properties are accessible only to the System Administrator role(s) of iRIS™.

11.100(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, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.

(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.

## **iMedRIS Statement**

This document, which is sent to the agency, should state – for each person – that the electronic signatures are to be considered as legally binding as traditional handwritten signatures. The document should be signed (handwritten signature) by the person in the organization who is responsible for maintaining the uniqueness and security of the electronic signatures. This is the responsibility of the client.

*(2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.*

## **iMedRIS Statement**

Such additional information shall be provided with the necessary information and in the format required by the agency (client). The agency may require this information to be notarized or externally certified in some other manner. This is the responsibility of the client.

## **Validation**

1. The client creates the Security Policy in System Administration.
2. If the Security Policy feature is turned on, users must agree to the security policy on initial login to iRIS™.

## **Electronic Signature Components and Controls**

### *11.200 Electronic Signature Components and Controls*

#### *11.200(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.*

## **iMedRIS Statement**

All accesses to iRIS™ require a unique user ID plus a specific password. All ID's are unique and each has the complete name of the owner associated with it in their user account. Login attempts, both successful and unsuccessful are recorded in the audit trail. Before executing a signature, the password must be confirmed. See example screenshot below:

Submission Signoff Sheet Back

Save Signoff

Study Title: test again

Submission Form(s): [Click here to review the submission documents](#)

Catherine Ackerman  
as Principal Investigator  
do you Approve or Deny this  
submission?  Approve  Deny

[Click here to add comments.](#)

This form requires your electronic signature. User ID:   
if Approved, Please enter your User ID & Password: Password:

**Investigator Assurance**

I am particularly aware that as an investigator conducting research sponsored by General Hospital, I assume certain responsibilities, namely that:

- The proposed research must meet scientific, ethical, and fiscal merit criteria before the actual work may begin;
- I will comply with all regulatory requirements and policies that govern the conduct of research at General Hospital;
- I will maintain accurate and -records of all work performed and results obtained;
- I will insure proper supervision of research personnel and data collected during the conduct of the study;
- I will insure appropriate dealings with industrial representatives and avoid any conflicts of interest;
- I will participate in the open publication and discussion of research methods and results and give appropriate assignment of credit and responsibility for research and publications.

### Validation

1. User ID
  - a. Unique for each instance of iRIS™
  - b. Associated to complete name of owner in user account
2. Login attempts
  - a. Recorded in system audits
  - b. Set system property to email system administrator after a client specified amount of failed login attempts
3. Apply signature
  - a. Must supply user ID and password before saving the signature
  - b. Password is confirmed before signature is applied to any document

(2) Be used only by their genuine owners.

### iMedRIS Statement

To execute the signing of the electronic record, the password must be confirmed. The client and its personnel are responsible for creating and securing user ID's and passwords.

### Validation

(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.

### iMedRIS Statement

To use an electronic signature, the person must be logged on as a user with one or more signature privileges. Each user should change their initial password immediately upon first log on. This prevents the administrator (the person that created the user account), from being able to log on as the genuine user.

### Validation

1. User must have a role as a Principal Investigator or other key study personnel (KSP) to apply a signature to a submission.

- a. Necessary signatures are defined in the workflow
- b. Users assigned PI or other KSP role in the study application form or in study management
  - i. Must have access to the study to assign these roles
2. User's signature must be specified as required by another, appropriate role within the system
  - a. If user is required to apply signature, only that user will receive the availability to do so
3. Set a system property to require a change of password on initial log on

*11.200(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.*

### **iMedRIS Statement**

The iRIS™ software application is not based on biometric identification but three distinct components: the user ID, the user's password and the user's role.

### **Validation**

1. User ID
  - a. Unique for each instance of iRIS™
  - b. Associated to complete name of owner in user account
2. Password
  - a. Associated to the user ID when applying the signature
3. Role
  - a. User must have a role as a Principal Investigator or other KSP to apply a signature to a submission.
  - b. User must be specified as required by other, appropriate role within the system
  - c. Signature access is granted based on department and/or review board access

### **Access Time-out**

*Concerning 11.200, the FDA in its comments in the Federal Register states (XII.124):*

*"The agency acknowledges that there are some situations involving repetitive signings in which it may not be necessary for an individual to execute each component of a non-biometric electronic signature for every signing, " ... " For example, an individual performs an initial system access on 'log on,' which is effectively the first signing, by executing all components of the electronic signature (typically both an identification code and a password)" ... " ...it is vital to have stringent controls in place to prevent the impersonation. Such controls include: (1) Requiring an individual to remain in close proximity to the workstation throughout the signing session; (2) use of automatic inactivity disconnect measures that would 'de-log' the first individual if no entries or actions were taken within a fixed short timeframe; and (3) requiring that the single component needed for subsequent signings be known to, and usable only by, the authorized individual."*

### **iMedRIS Statement**

User inactivity on the system for more than an administrator-specified period of time will automatically log off the current user. Log-offs are also recorded in the audit trail.

### **Validation**

1. Set the property `system.session_timeout_in_minutes` to the amount of idle time before user is prompted if they want to continue

- a. After the prompt is idle for five minutes before the user is logged off of iRIS™

system.session_timeout_in_minutes	40	<input type="checkbox"/> Check to encrypt permanently
<i>Description:</i> Depending on this setting, the system will open a pop up when the system times out, asking the user if they would like to stay logged into the system. Enter the amount of time, in minutes, that the system should timeout at.		

## Controls for Identification Codes/Passwords

11.300(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.

### iMedRIS Statement

Whenever the iRIS™ system administrator creates a new user account, the iRIS™ software validates each unique user ID and ensures that the user ID and password are not duplicated in the system. The password is also encrypted in the database for additional security. In addition, password and ID changes are time stamped and stored in the audit trail.

### Validation

1. New user ID, or a change in a user ID, cannot match the ID of another user. The system will not allow the save.
2. Encrypted password
3. Audit trail tracks user ID and password changes
4. Only the role of System Administrator has access

11.300(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g. to cover such events as password aging).

### iMedRIS Statement

Passwords can be set to automatically expire after a specified length of time after they were created.

### Validation

1. Set the property system.password\_expiration\_period for the amount of days to cycle password expiration.

system.password_expiration_period	1	<input type="checkbox"/> Check to encrypt permanently
<i>Description:</i> Set the amount of time for the password expiration period. The system will notify the user when the user logs on that their password has expired and it will ask them to create a new one.		

2. User is required to change the password after the amount of days has passed.
  - a. User cannot use the same password, it must differ

11.300(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.

## **iMedRIS Statement**

iMedRIS Data Corporation does not supply user ID's and/or passwords in the form of physical tokens, cards, or other devices.

### **Validation**

If the user or any other person believes that a password has been compromised, they should immediately inform their administrator and change their password immediately. In this case, the administrator may also choose to set up a new user account.

## **Unauthorized User Detection**

*11.300(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.*

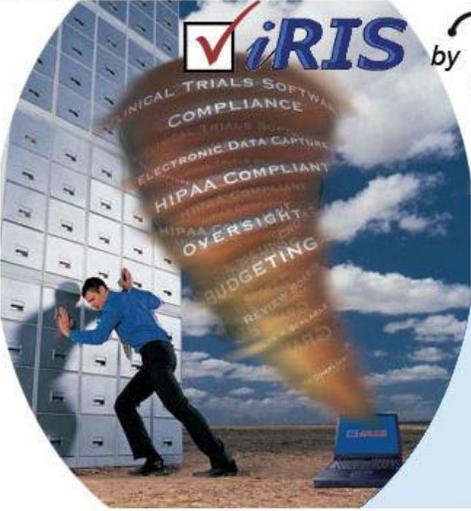
## **iMedRIS Statement**

As a measure of active prevention, each user should be trained to keep passwords secret and to change the password periodically. The iRIS™ software provides a password renewal/aging feature to assist the users in periodically changing their passwords. After a given period of time, which is determined by the administrator, the user will be automatically reminded to change the password. In this case, the password must be changed in order to log on and use the system. Three attempts are allowed for the user log on. Unsuccessful attempts to log on to the user level are recorded in the „System Audit Trail“. Also, after the administrator's specified number of failed log in attempts, the system will automatically generate an e-mail warning of potential security breach.

### **Validation**

Unsuccessful logon attempts will lockout further logon activity for a set period of time. Both the amount of unsuccessful logons and the period of time the user will be locked out are configurable by the System Administration role. The fact that the lockout occurred is recorded in the audit trail and notifications are emailed to all users with the System Administrator role.

**Log In**



**User ID:**

**Password:**

**Due to repeated failed logins, your account has been locked for 30 minutes**

[I forgot my Password](#) | [Request new account](#) | [System/Browser Requirements](#)

---

TEST

[Terms of Use](#) | [Privacy Statement](#)  
Copyright © 2001-2010 iMedRIS Data Corporation. All rights reserved.  
Version 8.02 Build 1510 Updated 1/11/2010