21 CFR 11 Validation Document for ERSA

Ochsner IRB’s Electronic Research Study Application

(Vendor: Huron)

Key references for this validation document
- FDA: http://www.fda.gov/regulatoryinformation/guidances/ucm125067.htm
- Vendor’s website: https://www.huronconsultinggroup.com/expertise/technology/click-portal-solutions

Requirements to be compliant with Part 11:
1. Technical controls. Click Commerce has provided IRB software, hereafter named ERSA, which contains the required technical components of a 21 CFR 11 compliant system. This document does not attempt to detail these. Contact the vendor for these details. Click Commerce asserts that this software meets these technical requirements.
2. Procedural Controls. These include notification, training, SOPs, administration. This ERSA 21 CFR part 11 validation document contains these, and also act as SOPs for the ERSA system.
3. Administrative Controls. These are controls put in place by the user beyond the technical controls provided by the vendor

All three of these controls are needed for overall part 11 compliance. The vendor provides the technical controls. This validation document provides or reviews the procedural and administrative controls.

Q: What software has to be part 11 compliant?
A: If the electronic system is source documentation for FDA required documents, then the system must be 21 CFR 11 compliant. ERSA must be part 11 compliant because it is the source documentation for many requirements in the FDA regulations, such as IRB applications, tracking approvals, etc.
Preface
By Nick Stier, Huron, formerly Click Commerce

Nick Stier is the Vice President of Business Development for Healthcare and Higher Education for Click Commerce, Inc. He can be reached at nicks@clickcommerce.com ©2005 Click Commerce, Inc., All rights reserved. This document was obtained from the vendor’s website

Compliance Automation Brief #1

Approval Processes, Security and 21 CFR Part 11

For anyone automating regulatory compliance document flows, there's clearly a challenge in defining what's required to conform to 21 CFR Part 11. In this brief, Webridge examines the application of Internet automation technologies, and 21 CFR 11 guidelines to IRB and Grant approval processes. This month we'll look at access-level security and what's practical to implement for an automated compliance or grant approval system. We think some access-level security technology far exceeds the practical needs for effective approval automation when combined with secured data transport such as Secured Sockets Layer (SSL) and your own Standard Operating Procedures (SOPs) for controlling physical access. We'll address transport-level security issues in a future brief with document security.

21 CFR 11 Review

Verification and auditing capability (auditability) are at the core of every approvals system: institutions must be able to prove that any person taking action with the system is who they say they are. Furthermore, document submissions, reviews and approvals must be recorded reliably and cannot be changed without documentation: electronic signatures are key to achieving this. The issues here really boil down to how much access security is satisfactory given the environment in which the system operates, whether "open" or "closed".

Closed System Policies and Access Security

A discussion about security should begin with the assumptions about the system operating environment. In the case of an approvals management system, the assumption is that the system is "closed": e.g. that the grant applications or research proposals and associated approval document data would be maintained within the same institution who is governing the process. Closed systems address some of the data integrity and confidentiality issues through an assumed level of trust among employees that is backed up with SOPs. For example, an SOP might forbid employees from writing down system passwords on notes near their workstations while, in parallel the automation system policy might require rotating to a new password every 30 days. Both work together to ensure data integrity and confidentiality.

With Internet technologies such as browsers and servers with extranet security, it's now possible for external companies, such as sponsors or commercial IRB personnel, to play a role in approval processes. Document and content security make it easily possible to accommodate external participants while hosting the system centrally within the Institution and still maintain a "closed" system context. But, exactly what should be the access security for such a system and how
Different from an "open" system where 21CFR Part 11 requires stronger authentication involving digital signatures, a closed system might use a combination of identification code (name)/password pairs as well as multiple passwords for certain electronic signature actions. Note the distinction between "digital signatures" and "electronic signatures"; some security technologies that implement the formers—several of which are still unproven—present cumbersome usage and cost challenges. Reviewing each starting from the low end:

- **Name/password**: the most widespread authentication scheme for electronic signatures, this scheme has the advantage of being familiar to anyone who has ever touched a computer. When abutted by SOPs that ensure proper password administration and conscientious employee use, name/password schemes provide an appropriate first-level of system access and operation.

- **Multiple passwords**: adding a "signature" password for comments, changes and approvals provides protection against careless or deliberate unauthorized use of the system. After signing-in with a system-wide password, certain creation, modification or approval actions require the use of a second password before the system will record the user's action. Adding complexity to the administration and usage process, multiple passwords now must be rotated on a similar basis to the conventional ones, but to a different audience of users who, for their part, need to confidentially retain a second key. More involved for everyone, but definitely manageable.

- **Public Key Infrastructure (PKI) authentication**: PKI document encryption with private and public keys is arguably the most comprehensive and secure means of ensuring the identity of an author and tying it irrefutably to a singular edition of a document. However, PKI technology also complicates system design, performance and user experience. With digital certificates, users are typically tied to their workstations for...
signing operations, which eliminates the cost advantages of universal browser access: each time a user wishes to work from a different machine, a process to transfer the certificates to the new machine adds complications. In addition, like passwords, the loss or theft of a private key can result in impersonation. Finally, additional care must be used in determining the performance characteristics of a system where thousands of users are taking actions involving digital certificates: authentication traffic involving public/private key decoding can present significant computing overhead. Pilot testing the use of PKI on a small population of users would seem to be a prudent means of observing its characteristics (and costs) before widespread roll-out in a production setting.

- Biometric identification: using physical data as an authentication means continues to raise legal questions as well as questions of efficacy. Fingerprint, facial scans, voice recognition technologies have repeatedly gained press for spectacular failures. For example, read this recent BBC article: http://news.bbc.co.uk/hi/english/sci/tech/newsid_2016000/2016788.stm. Also, with the costs involved in adding hardware, it seems likely that biometric identification's adoption will be limited to applications where multiple means of verifying identity are required (e.g. military or national security applications).

- Future: the legal issues of collecting biological identity data aside, at some point in the future, hardware costs for effective biometric monitors may come down and PKI issues eased with the familiarity that comes from widespread exposure. At that time, the distinctions between authentication for closed and open systems may well blur as costs and usage difficulty become insignificant.

Summary

An Institution must choose the right technologies that encourage automation system adoption by the constituents who need it most: the PIs, the IRBs and Department personnel. Security for any approvals system is a constant decision-making process that must balance SOPs for physical system access with the use of appropriate, available electronic technologies that resist breach, but encourage easy-to-use steady-state operation. Excessive electronic safeguards on a closed system can add expense, complicate deployment and retard user acceptance.
1. Introduction
   
   A. This validation document shows how the software system was validated to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.
   
   B. History & Purpose of the software

2. Validation\(^1\)
   
   A. Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.
   
   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.
   
   C. Protection of records to enable their accurate and ready retrieval throughout the records retention period.
   
   D. Limiting system access to authorized individuals.
   
   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.
   
   F. Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.
   
   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.

---

\(^1\) 21 CFR 11 section 11.10 ([http://frwebgate.access.gpo.gov/cgi-bin/get-cfr.cgi?TITLE=21&PART=11&SECTION=10&YEAR=2002&TYP](http://frwebgate.access.gpo.gov/cgi-bin/get-cfr.cgi?TITLE=21&PART=11&SECTION=10&YEAR=2002&TYP)) gives the sections of this Chapter
H. Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

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.

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.

K. Use of appropriate controls over systems documentation including:
   i. Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.

      ii. Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

3. User Training & Documentation

   A. Training sessions for front and back end users

   B. Help Screens built into the software

   C. User manual for front end users

   D. User manual for back end users

4. Appendix

   A. Ochsner polices that affect ERSA
Validation Documentation

1. Introduction

   A. Document Purpose
      i. This validation document shows how the software system was validated to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. The technical controls are deferred to the vendor, Huron. This document focuses on the procedural and administrative controls that are the responsibility of the local institution.

   B. History & Purpose of the software
      i. Development timetable. The ERSA system went through initial modification for Ochsner in early 2005, then was alpha and beta tested in the Spring of 2005. On July 5, 2005 it was deployed throughout the institution for IRB applications, with the expectation it would take many months to fine tune all aspects, and it would take about 15 months to enter all studies. Due to inaccuracies in the previous CIS database, it was decided not to port over any information to ERSA from CIS. Instead, all new studies would be entered into ERSA, and old studies would start using ERSA with their next continuing review. The ERSA system was in use for all studies by 2007. Old studies that were closed prior to needing a continuing review that must be done in ERSA were not archived in ERSA. Major system updates issued by the vendor were implemented in the years since. As of Nov 2016 the Huron Click version 8.0 was being planned on for implementation in 2017.

      ii. Code development & reliability testing. This is done by the vendor, and as of Nov 2016 was supplemented by consultants (Bad Rabbit, Inc.)

2. Validation

   A. Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. This is a technical control provided by the vendor. Alpha and beta testing was done to assure no problems were found. Whenever questions about these areas arise, the vendor is consulted for a diagnosis and fix of a problem if found.

   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

---

2 21 CFR 11 section 11.10 (http://frwebgate.access.gpo.gov/cgi-bin/get-cfr.cgi?TITLE=21&PART=11&SECTION=10&YEAR=2002&type=text) gives the sections of this Chapter
questions regarding the ability of the agency to perform such review and copying of the electronic records. This is a technical control provided by the vendor. Alpha and beta testing was done to assure no problems were found. Whenever questions about these areas arise, the vendor is consulted for a diagnosis and fix of a problem if found. Whenever government auditors find the ability of the system lacking for their requirements, the vendor will be consulted to obtain a fix.

C. Protection of records to enable their accurate and ready retrieval throughout the records retention period. The ERSA database system has records stored on a server at Ochsner. There is a backup server located at Ochsner. Backup happens nightly automatically and is scheduled by the Information Services Department (ISD). In the event of an imminent disaster, the server can also be backed up by Huron offsite on their server in Oregon. This is decided by the IRB Administrator in conjunction with the Vice President of Research.

D. Limiting system access to authorized individuals. The ERSA system requires a username and password to access it. Only the IRB Administrator or designee may issue these. They are only issued to individuals who have completed the required human subject protections training set by the institution.

The institution has Policy OHS.IS.008 Data Access Control, the full policy is at the end of this document, and says in part:

User Responsibilities:
1. User IDs must not be shared or used by anyone other than the user to whom they are assigned. Users are accountable for all activity associated with their assigned User IDs.
2. Passwords should not be the equivalent of a user’s personally identifiable information such as social security number, driver’s license number, names of family members, etc. The use of pass-phrases is recommended as outlined in the definition section of this policy.
3. Passwords must not be displayed or easily found.
4. Passwords must be changed immediately if the user knows or suspects disclosure or unauthorized use.
5. Each user must activate a password protected screen lock if they temporarily leave a computer workstation with an application (i.e. EPIC) logged on; otherwise, they must terminate their individual application session (logoff).
6. Users must not operate the workstation under someone else’s application login credentials. If a user needs to use an unattended and unlocked workstation application session, they must login to start their own application session.
7. Users must not by default save ePHI and/or other confidential data on their computer’s hard drives.
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 required for the subject electronic records and shall be available for agency review and copying. This is a technical control provided by the vendor. Alpha and beta testing was done to assure no problems were found. Whenever questions about these areas arise, the vendor is consulted for a diagnosis and fix of a problem if found.

F. Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate. The ERSA system workflow process was set up after extensive consultation between the vendor and the institution’s IRB and IS departments. All the sequences of steps are consistent with the regulations. Whenever questions about these areas arise, the IRB Administrator and ISD meet to discuss and work out a solution consistent with the regulations. When necessary, the vendor is consulted for a diagnosis and fix of a problem that cannot be resolved locally.

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. The ERSA system can only be accessed by those individuals who have received an ERSA username and password from the IRB Administrator or designee. Once an individual is logged into the system, their audit trail identifies them and what they have done. Ability to perform functions and access information is tailored to the security and role of the individual.

H. Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction. Because the ERSA system’s data input consists solely of people typing in data via keyboards and confirming the accuracy of their input by looking at the screen, there is no need for additional device checks for data input. The only data output would be screen shots and printouts of the documents within the ERSA system. All users of the ERSA system are already well experienced in word processing and computer entry issues.

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. ERSA has built in help text to to provide training how to use the system as needed. Only the IRB Administrator or designee can issue these. See 3A below.

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. This validation
document, along with the statements in ERSA, are the IRB’s written policy that holds an individual accountable and responsible for actions initiated under their electronic signature in ERSA. When a user logs into ERSA, the login includes the following statement, “After signing into this site, you are bound by the terms and conditions set forth when you received your account.” See part 3 for user education and training. Ochsner’s policy on passwords applies to all of the institution’s electronic databases including ERSA. During the course of an IRB application the clinical research coordinator, the principal investigator, and the sub-investigators all must access the ERSA system to do various functions. These are subject to the Ochsner Data Access Control Policy about passwords which is copied in full at the end of this document.

K. Use of appropriate controls over systems documentation including:
   i. Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. No one can access the system unless the IRB Administrator or designee issues a username and password. See parts 3C and D below for user manuals that document system operation. Maintenance of the system in terms of upgrades and fixes when required are provided by the vendor. Process flow within the system is maintained and adjusted by the IRB Administrator and ISD who are the site managers for the system.

   ii. Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation. This is a technical control provided by the vendor. Alpha and beta testing was done to assure no problems were found at our site. Whenever questions about these areas arise, the vendor is consulted for a diagnosis and fix of a problem if it found. ERSA has been designed so that all changes are transparent, that is, they are listed in the study window along with who made the change, and the date. Older versions are never erased, and are always available for viewing.

3. User Training & Documentation

   A. Training sessions for front and back end users. The front end users have training guidance documents available at https://ersa.ochsner.org. Training sessions will be scheduled as needed from time to time. These are also incorporated into the CRC Orientation Training Modules that are required of all new CRCs and can be attended as a refresher by anyone who wishes. Back end users in the IRB Office get on the job training using the same guidance documents and additional information from the IRB Administrator.

   B. Help Screens built into the software. Help text is built in throughout the ERSA screens. It defines terms, and explains what to do at each step. This help text is extensive, and provides users most of the information needed to accurately and properly fill out the IRB application.
4. Appendix
   A. Ochsner polices that affect ERSA. The following polices were the most relevant in force at the time of the current version of this validation document (see footer). The institution’s Intranet site has the most current policies in force.


I. Purpose
The purpose of this Policy is to comply with Food and Drug Administration (FDA) regulations that ensure the integrity, trustworthiness, and reliability of Electronic Records and Electronic Signatures used in FDA regulated research studies.

II. Scope
   A. Principal Investigators must ensure that electronic records used in support of FDA regulated studies are compliant with FDA 21 CFR 11 rulings.
   B. Records considered by FDA as electronic source documents include:
      1. Hospital records,
      2. Clinical and office charting,
      3. Laboratory notes and Laboratory records,
      4. Memoranda,
      5. Subjects diaries or evaluation checklists,
      6. Pharmacy dispensing records and other records
      7. Recorded data from automated instruments,
      8. Copies or transcripts certified after verification as being accurate and complete, and
      9. Microfilm, X-rays, Imaging, Magnetic imaging

III. Definitions
   A. 21 CFR 11: This rule provides the electronic record and electronic signature criteria for FDA regulated research where data is created, modified, maintained or transmitted electronically.
   B. System Administrator: One who has primary accountability for a computer system.

IV. Policy Statements
   A. Computerized systems that process electronic source documents in support of FDA regulated human subject research must have administrative, procedural, and technical controls in place according to requirements of FDA 21 CFR 11 for electronic records and if used, electronic signatures
   B. Any new system which comes under the scope of this Policy must be evaluated for 21 CFR 11 compliance before being placed into a production environment.

V. Procedures/Standards and Roles & Responsibilities
A. System administrators must document compliance with 21 CFR 11 by using the 21 CFR 11 System Validation Form. Electronic copies of completed/updated assessments must be forwarded to compliance@ochsner.org.
B. System administrators must periodically re-asses their systems for 21 CFR 11 compliance.
C. Principal Investigators (PI’s) must forward all sponsor requests regarding 21 CFR 11 to Compliance and Privacy. Along with the sponsor request, PI’s must complete the attached Request for Completion of Sponsor’s Electronic Records/Electronic Signature Assessment form and send both to Compliance and Privacy by faxing (504-482-6106) or by e-mailing to compliance@ochsner.org.
D. Compliance and Privacy will complete the sponsor requests and return a copy to the Principal Investigator.
E. Corporate Integrity will centrally file copies of all correspondence and questionnaires in regards to 21 CFR 11 validation.

VI. Enforcement and Exceptions
Failure to comply with the 21 CFR 11 Electronic Data Capture and Electronic Signature Policy may result in disciplinary action up to and including termination of employment for employees or termination of contract for contractors, partners, consultants and other entities.

VII. Internal References
Request for Completion of Sponsor’s Electronic Records/Electronic Signature Assessment Form
21 CFR 11 System Validation Form

VIII. External References
FDA 21 CFR 11 Ruling

IX. Policy History
8042-6, Electronic Data Capture 21 CFR Part 11 Compliance for FDA Regulated Studies (21 CFR 11)

X. Approved
Warner Thomas, President and Chief Executive Officer
Michael Hulefeld, Executive Vice President and System Chief Operating Officer
William W. Pinsky, M.D., Executive Vice President and Professional Affairs Chief Academic Officer

Policy OHS.IS.008 Data Access Control

I. Purpose
The purpose of this policy is to control access to Ochsner’s electronic systems and data. These rules are necessary to preserve the integrity, availability, and confidentiality of ePHI and other confidential information.

II. Scope
Employees, contractors, part-time and temporary workers and those employed by others to perform work on Ochsner Health System (OHS) premises or who have been granted access to and use of OHS information assets are covered by this policy and must comply with associated standards and procedures.

III. Definitions:
   A. Confidential - is the classification designated for company information assets that create, receive, store, or transmit electronic protected health information (ePHI) and/or sensitive information assets that if disclosed could be used to cause hardship, embarrassment or harm to Ochsner patients, employees or other customers.
   B. Electronic Protected Health Information (ePHI) - under HIPAA means any electronic protected health information that identifies an individual.
   C. Information Assets - Hardware or software that creates, receives, stores or transmits electronic data used for patient care, clinical research or in support of Company business processes; including all data maintained or accessed through systems owned or administered by or on the behalf of the Company.
   D. Pass-phrase – A technique for generating a difficult to guess password. For example, using the first letter of a word in a sentence that has meaning only to the user and including special characters/numbers/etc as demonstrated below:
      A passphrase is similar to a password, but is more complicated for someone else to guess. It is usually generated using the first letter (or substitute) of a phrase that means something only to you. For example, “To be or not to be?” could become 2BRnot2B? (Please don’t use this particular passphrase)
   E. System Administrators - Are the custodians of the system as assigned by the system owner/s. Those designated by the system owner to manage process or store information assets.

IV. Policy Statements
   A. Data access controls must be implemented to protect ePHI and/or other confidential data from unauthorized view and/or modification.
   B. Authorization to data and applications must be made on a need to know basis to perform a specified job related task, function, or role.

V. Standards and Roles & Responsibilities
   A. Standard: OHS is adopting the Payment Card Industry (PCI) password standard.
      1. Passwords must have a minimal length of seven characters.
      2. Passwords must contain both numeric and alphabetic characters.
      3. Passwords must be changed every 90 days.
      4. New passwords cannot be the same as the last four passwords.
      5. User account is locked after five consecutive incorrect password attempts.
      6. Passwords must not be equal to or a derivative of the User ID
   B. Management Responsibilities:
      1. User access must be restricted to the information assets required to meet an approved business need or perform prescribed job responsibilities (limited need to know basis).
2. Third parties must sign a statement to maintain confidentiality of Ochsner data or be covered under a Business Associate Agreement before obtaining access to ePHI and/or other confidential data.
3. Contractors and temporary employees accessing ePHI and/or other confidential data, or systems supporting ePHI/confidential data, must have individual user id’s and passwords with an account expiration date that coincides with the anticipated end of employment or contract. The default account expiration date for temporary user-ids must be set to 90 days if the length of service is not known.

C. User Responsibilities:
1. User IDs must not be shared or used by anyone other than the user to whom they are assigned. Users are accountable for all activity associated with their assigned User IDs.
2. Passwords should not be the equivalent of a user’s personally identifiable information such as social security number, driver’s license number, names of family members, etc. The use of pass-phrases is recommended as outlined in the definition section of this policy.
3. Passwords must not be displayed or easily found.
4. Passwords must be changed immediately if the user knows or suspects disclosure or unauthorized use.
5. Each user must activate a password protected screen lock if they temporarily leave a computer workstation with an application (i.e. EPIC) logged on; otherwise, they must terminate their individual application session (logoff).
6. Users must not operate the workstation under someone else’s application login credentials. If a user needs to use an unattended and unlocked workstation application session, they must login to start their own application session.
7. Users must not by default save ePHI and/or other confidential data on their computer’s hard drives.

D. System Administrator Responsibilities:
1. Must disable user access upon notification of termination or end of contract for individuals.
2. All systems must require and authenticate a valid User ID and password/token prior to granting access to network or system resources and applications.
3. Each user must have a unique account identifier/user id.
4. Generic User IDs may be used to boot-up a multi-user workstation as long as the userid/account is not accessing ePHI and/or other data classified as sensitive/confidential.
5. Given/temporary passwords on new accounts must expire upon first log-in and require an immediate password change.
6. Proper identification procedures must be developed and followed to authenticate users before re-setting or re-activating passwords.
7. Passwords to default system accounts must be changed before being placed into a production environment or connecting to the Ochsner network.
8. The number of concurrent log-ins allowed per User ID should be restricted to the minimum number required to perform a given job function.
9. All systems must log the date and time of all failed and successful user attempts to access the systems containing ePHI and/or other confidential data.
10. Privileged accounts are only to be used when performing specific actions that require an elevated privilege level.
11. Authentication credentials (e.g., User IDs and passwords) must not be stored in readable form in automatic log-in scripts, software macros, terminal function keys, computers without access control, shortcut files or other locations where unauthorized persons might discover them.
12. Authentication data (e.g. password files) must be protected with encryption controls to prevent unauthorized individuals from obtaining the data.
13. User IDs that are unused, dormant or inactive must be disabled.
14. System Administrators must have provisions for allowing emergency access, emergency id’s and passwords, when no other means of emergency solution is available.
15. Procedures must be documented for granting and logging special access privileges during an emergency situation (for example, to fix a time-sensitive production problem).
16. After emergency situations, special access privileges must be disabled.
17. System Administrators must perform at least annual reviews of access profiles to ensure only authorized users are allowed access to ePHI and/or other confidential data and that access is granted on a need to know basis.

VI. Enforcement and Exceptions
A. Requests for exceptions to the Data Access Control Policy must be submitted in writing to the Chief Information Officer, CIO, and the General Counsel & Sr. Vice President of Corporate Compliance and must:
   1. Describe the reason for requesting an exception.
   2. Describe the specific impact on workflow process or patient care if request is denied.
   3. Describe any system limitations causing compliance issues with this Policy along with any future plans to address.
B. Requests for exceptions will be answered in writing within 30 days of receipt of the request, approving, denying, or requesting additional information.
C. Failure to comply with the Data Access Control Policy may result in corrective action in accordance with the HR Progressive Discipline policy and/or termination of contract.

VII. Internal References
[This section intentionally left blank]

VIII. External References
HIPAA Security Rule 164.308(a) (4)(ii) (B) Information Access Authorization
HIPAA Security Rule 164.308(a)(4)(ii)(C) Access Establishment and Modification
HIPAA Security Rule 164.308(a)(5)(ii)(d) Password Management

IX. Policy History
8480-1 Computerized Information Access

X. Approved
Warner Thomas, President and Chief Executive Officer
Michael Hulefeld, Executive Vice President and System Chief Operating Officer
Douglas Lauterbach, Interim Chief Information Officer