Standard Operating Procedure –

Information Security Compliance Requirements under the caBIG™ Program

This cover sheet controls the layout and components of the entire document.

Issued Date: October 30, 2006

Effective Date: December 11, 2006

Department Approval:

Peter Covitz

Chief Operating Officer, NCICB

QA Approval:

George Komatsoulis

Director of Quality Assurance

Note: This document will be issued for training on the Issue Date. The document will become available for use to trained personnel on the Effective Date. Before using this document, make sure it is the latest revision. Access the caBIG™ website to verify the current revision.

Revision History

Revision	Date	Author	Change Reference	Reason for Change
1.0	09/19/2005	SOP Working Group	N/A	Initial release.
2.0	10/30/2006	BP SIG/SOP WG	All pages	Annual update.

1. Purpose

The purpose of this standard operating procedure (SOP) is to describe the information security responsibilities of caBIG™ participants with access to systems maintained by the National Cancer Institute Center for Bioinformatics (NCICB). The procedures are designed to assure that institutional security practices are consistent with the *Secure One HHS Information Security Program Policy*, *Secure One HHS Information Security Program Handbook*, and federal legal requirements; and compatible with the Security Rule of the Health Insurance Portability and Accountability Act (HIPAA), which applies to many cancer centers. This Standard Operating Procedure will ultimately facilitate collaborative research efforts among cancer centers and other institutions.

2. Scope

This SOP advises all caBIG™ participants having access to applications supported by the NCICB on the minimum steps that are required to assure the security of patient data submitted to, and provided by, the these applications. Participating institutions should identify and implement any and all other security measures deemed reasonable and necessary to protect the confidentiality, integrity, and availability of any information they send, receive, use, or store using the applications within the NCICB environment. Cancer centers and other institutions that access NCICB applications and that are covered entities under the HIPAA Security Rule must maintain compliance with the policies and procedures required by the Rule, and all cancer centers must identify and implement all reasonable and appropriate policies and procedures for ensuring information security. Participating cancer centers and other institutions should address all the items contained within this procedure in order to demonstrate good faith measures have been taken to reduce the risk of a security breach and to mitigate possible consequences of a compromise of information security. Participating cancer centers and other institutions understand and accept that addressing this SOP alone will not constitute compliance with the HIPAA Security Rule.

3. Requirements

3.1 All cancer centers and other institutions seeking access to the caBIG™ applications and environment should maintain comprehensive policies to prevent, detect, contain, and correct security violations consistent with the HIPAA Security Rule (HIPAA Security Rule §164.308(a)(1)(i)) and the *Secure One HHS Information Security Program Policy*. Policies may be incorporated into any existing information security policies maintained by the cancer centers or other institutions, or policies specific to the NCICB applications may be developed and implemented, as needed. Security policies should minimally include, but may not be limited to, the following provisions:

3.1.1 A policy that states that individuals will only be given access to those projects and records that are necessary for them to perform their specific research projects or other assigned duties, consistent with the HIPAA Security Rule (§164.308(a)(3)(i)) and the *Secure One HHS Information Security Program Policy*, Section 4.1.6 (“Least Privilege”).

3.1.2 A policy for formally authorizing individuals to request access to the NCICB application(s) from the NCICB Applications Support team and for supervising user access once it is rewarded.

3.1.3 A policy defining the approach to be employed by each cancer center and other institution in conducting background, reference, qualifications, and/or performance evaluation checks of users who will have access to the applications. This policy should state what reasonable and necessary steps will be taken to verify that access granted to users is appropriate to the individual user's expected use of the clinical data management system, individual qualifications and experience, and when reasonable and necessary, the user's prior performance or other relevant background. Each cancer center and other institution should provide the stated assurances documentation to the NCICB Applications Support team along with the request for authorizing individuals' access to the caBIG™ environment. (See the *Secure One HHS Information Security Program Policy*, Section 3.2 ("Contractors and Outsourced Operations") and the *Secure One HHS Information Security Program Handbook*, Section 3.2 ("Contractors and Outsourced Operations").

3.1.4 A policy for terminating an individual's access to the NCICB systems when employment terminates or work responsibilities are no longer required access to the caBIG™ environment. (See the *Secure One HHS Information Security Program Policy*, Section 4.1.8 ("Personnel Separation") and the *Secure One HHS Information Security Program Handbook*, Section 4.1.8 ("Personnel Separation")).

3.1.5 A policy limiting physical access to the facilities where the NCICB systems can be accessed, consistent with HIPAA Security Rule §164.310(a)(1) and the *Secure One HHS Information Security Program Policy*, Section 4.2 ("Physical Security").

3.1.6 A policy forbidding circumvention of any technical security measures of the NCICB systems (HIPAA Security Rule §164.312(e)(1) and the *Secure One HHS Information Security Program Policy,* Section 4.1 ("Personnel Security")).

3.2 All cancer centers and other institutions seeking access to the NCICB clinical data management systems environment should maintain comprehensive procedures to prevent, detect, contain, and correct security violations consistent with the HIPAA Security Rule (HIPAA Security Rule §164.308(a)(1)(i)), the *Secure One HHS Information Security Program Policy, and* the *Secure One HHS Information Security Program Handbook* . Security procedures should address the following required practices:

3.2.1 Implementing security policies, including but not limited to, those described in Section 3.1 of this SOP.

3.2.2 Identifying the person(s) responsible for assuring that information security practices relative to NCICB systems environment are consistent with this SOP and identifying those individuals who will be available as the chief Point of Contact (POC) for the National Cancer Institute (NCI) Information System Security Officer for the CABIG™ environment (Application ISSO).

3.2.3 Implementing a security awareness and training program for all workforce members, including members of management, who will access the caBIG™ environment (HIPAA Security Rule

§164.308(a)(5)(i) and the *Secure One HHS Information Security Program Policy*, Section 4.1.7 "Security Education and Awareness"). Security awareness and training can be incorporated into previously existing employee security training or other employee training programs.

3.2.4 Reporting promptly any suspected or confirmed breach of computer security to the NCI CSO, such as an unexplained loss of access to the NCICB clinical data management systems, alteration or disappearance of data stored on the system, discovery of intentional disclosure of protected information, or other significant violation of security policies, procedures, or legal requirements related to information security occurring at any cancer center, other institution or at the NCICB. (See the *Secure One HHS Information Security Program Policy*, Section 4.9, "Contingency Planning").

3.2.5 Informing the NCICB Applications Support team of any subcontractors or other outside entities who require access to the caBIG™ environment, consistent with HIPAA Security Rule §164.308(b)(1). The same policies, procedures, and responsibilities for implementing the security policies described in this SOP are expected of all subcontractors or outside entities that require access to the caBIG™ environment. (See the *Secure One HHS Information Security Program Handbook*, Section 3.2, "Contractors and Outsourced Operations").

3.2.6 Deleting information obtained from the caBIG™ environment (systems database and software) from hardware and electronic media prior to disposing of these resources or reassigning them to a different use (HIPAA Security Rule §164.310(d)(1) and the *Secure One HHS Information Security Program Policy*, Section 4.4.3, "Sanitation and Disposal of Information").

3.3 All cancer centers and other institutions seeking access to the caBIG™ environment will agree to cooperate with NCICB requests for assistance in maintaining current records and preparing necessary information security records and reports. These records and reports may include the following:

3.3.1 Records of users with access to applications in the caBIG™environment.

3.3.2 Evaluations of individual cancer center's and institution's security policies and procedures related to the caBIG™ environment.

3.3.3 Assessments of risk to the caBIG™ environment, including risk of compromises of computer security through unauthorized access ("hacking"), inappropriate use, or unintentional misuse (HIPAA Security Rule §164.308(a)(7)(i) and the *Secure One HHS Information Security Program Policy*, Section 3.7, "Risk Management").

3.3.4 Investigations of computer security incidents such as inappropriate access, misuse of data, unauthorized disclosure of protected information, consistent with the HIPAA Security Rule (§164.308(a)(6)(i)) and the *Secure One HHS Information Security Program Policy*, Section 4.9.1, "Security Incident and Violation Handling").

3.3.5 Periodic reports to the Secretary of Health and Human Services, Congressional committees, or other state or federal government agencies, as required by statute or regulation.

3.4 The NCICB Information System Security Officer will be responsible for the implementation and enforcement of the information security program, consistent with NCI, NIH, HHS and other applicable Federal Information System Security and Information Resources Management Policies.

The application ISSO shall serve as a point of contact and resource for cancer centers that are HIPAA covered entities, and shall assist them in coordinating their HIPAA Security Rule compliance programs with reference to the caBIG™ environment systems use and operation. (see the HIPAA Security Rule §164.308(a)(2)).

3.5 The NCICB will comply with policies and procedures to prevent, detect, contain, and correct security violations related to the caBIG™ systems, as required by the *Secure One HHS Information Security Program Policy*, the *Secure One HHS Information Security Program Handbook,* and any other relevant Federal laws, regulations, and/or guidance. Consistent with this guidance, NCICB will:

3.5.1 Coordinate with the application ISSO to ensure that NCICB implements all of its requirements under this SOP in compliance with established HHS, NIH and NCI security requirements.

3.5.2 Distribute system rules of behavior relevant to accessing and using the NCICB systems, consistent with the Secure One HHS Information Security Policy, to all NCI staff and the staff of cancer centers, and institutions that will access the caBIG™ environment (as required by the *Secure One HHS Information Security Program Handbook*, Section 4.1.2, "Rules of Behavior", and the *Secure One HHS Information Security Program Handbook, Appendix G, "Rules of Behavior"* (see especially *"Media Control"*)).

3.5.3 Review, documenting and modifying user rights for access to the caBIG™ environment to ensure compliance with this SOP; the *Secure One HHS Information Security Policy*, Section 5.2, "Access Control," and the *Secure One HHS Information Security Handbook*, Section 5.2, "Access Control."

3.5.4 Enforce a disciplinary action for the users who fail to comply with security policies and procedures, as required by the *Secure One HHS Information Security Policy*, Section 4.1.3, "Disciplinary Action" and the *Secure One HHS Information Security Handbook*, Section 4.1.3, "Disciplinary Action."

3.5.5 Inform cancer centers and other institutions that access caBIG™ environment of HHS' policy, procedures and contact information for reporting and addressing security incidents involving the use of the caBIG™ environment, as contained in the *Secure One HHS Information Security Program Policy* Section 4.9.1, "Security Incident and Violation Handling" and the *Secure One HHS Information Security Program Handbook* Section 4.9.1, "Security Incident and Violation Handling," and *Appendix G, "Rules of Behavior"* (see especially *"Incident Reporting Escalation"*).

3.5.6 Conduct an assessment of potential sources of threats to the security of the caBIG™ environment, possible vulnerabilities the system has to those threats, and identify reasonable and appropriate mitigations for those threats as required by the *Secure One HHS Information Security Program Policy*, Section 3.7.3, "Risk Assessments" and the *Secure One HHS Information Security Program Handbook*, Section 3.7.3, "Risk Assessments."

3.5.7 Document and implement proper backup procedures for information residing in the caBIG™ environment, and develop procedures to test backup via restoration of information from backup media, as required by the Secure One HHS Information Security Program Policy, Section 4.9.3, "Backup Data" and the Secure One HHS Information Security Program Handbook, Section 4.9.3, "Backup Data."

3.5.8 Conduct a self-assessment of the policies, procedures and practices used to protect the information collected by, residing on, and transmitted by the caBIG™ environment at least annually in accordance with the National Institute of Standards and Technology's (NIST's) Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*, as required by the *Secure One HHS Information Security Program Policy*, Section 3.9, "Self-Assessments," and the *Secure One HHS Information Security Program Handbook*, Section 3.9, "Self-Assessments,"

3.5.9 Provide physical protections for the servers and other architectural elements of the caBIG™ environment, including reasonable limitations of physical access to terminals on which the system may be accessed, as required by the *Secure One HHS Information Security Program Policy*, Section 4.2, "Physical Security" and the *Secure One HHS Information Security Program Handbook*, Section 4.2, "Physical Security".

3.5.10 Develop Standard Operating Procedures (SOPs) for the caBIG™ system applications that specify their functions and how they may permissibly be used, including descriptions and functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of specific workstations that access the application, as required by the *Secure One HHS Information Security Program Policy*, Section 4.8, "Equipment Security," and the *Secure One HHS Information Security Program Policy*, Section 4.8, "Equipment Security".

3.5.11 Ensure that information obtained from the caBIG™ systems, as well as the software, is deleted from hardware and electronic media prior to disposal in a manner that prevents unauthorized persons from using it as required by the *Secure One HHS Information Security Program Policy*, Section 4.4.3, "Sanitization and Disposal of Information" and the *Secure One HHS Information Security Program Handbook*, Section 4.4.3, "Sanitization and Disposal of Information."

4. References /Regulations/Guidelines

Section	SOP Number	SOP Title
4.1	N/A	Health Insurance Portability and Accountability Act (HIPAA) Security Rule
4.2	N/A	CDISC Glossary
4.3	N/A	SOP WG Glossary

Section	SOP Number	SOP Title
4.4	N/A	Title 21 CFR Part 11
4.5	N/A	Secure One HHS, Information Security Program Policy (December 15, 2004)
4.6	N/A	Secure One HHS, Information Security Program Handbook (December 15, 2004)
4.7	AD-005	SOP for Protecting Patient Privacy
4.8	CV-001	SOP for Complying with 21 CFR Part 11 [Electronic Records & Electronic Signatures – Regulated Systems] for the caBIG Program at the National Cancer Institute
4.9	IT-001	SOP for Establishing and Maintaining the User Accounts
4.10	IT-002	SOP for Retiring the User Accounts

5. Roles & Responsibilities

Role	Responsibility
NCICB Applications Director	• Maintain comprehensive program to implement policies and procedures to prevent, detect, contain, and correct security violations consistent with the HIPAA Security Rule 164.308(a)(1)(i)). • Create and enforce a policy of least privileges and need to know access controls for members of the workforce (HIPAA Security Rule 164.308(a)(3)(i)). • Implement security policy for evaluating access needs and authorizing access to the caBIG™ environment consistent with the HIPAA Security Rule (HIPAA Security Rule 164.308(a)(4)(i)). • Implement a security awareness and training program, in conjunction with security staff, for all workforce members, including members of management, who will access the NCICB clinical data management systems (HIPAA Security Rule 164.308(a)(5)(i)). • Provide NCICB with any information needed for NCICB to conduct a risk assessment on the caBIG™ systems (HIPAA Security Rule 164.308(a)(7)(i)).
NCICB Information System Security Officer (Application ISSO)	• Develop workstation user manuals that specify proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of specific workstations that access the caBIG™ systems, consistent with the HIPAA Security Rule (HIPAA Security Rule 164.310(b)). • Develop and implement policies and procedures to assure that information obtained from the caBIG™ systems, as well as the

Role	Responsibility
	software, is deleted from hardware and electronic media prior to disposal (HIPAA Security Rule 164.310(d)(1)). • Enforce the password protection policies and procedures to identify workforce members who are authorized to access the caBIG™ systems (HIPAA Security Rule 164.312(d)). • Implement and prevent the circumvention of any technical security measures of the caBIG™ systems (HIPAA Security Rule 164.312(e)(1)). • Implement and enforce security policies and procedures for reporting and addressing security incidents involving the use of the caBIG™ systems (HIPAA Security Rule 164.308(a)(6)(i)). • Cooperate with CIO in supplying any information needed to perform a periodic technical and non-technical security evaluation of the caBIG™ systems (HIPAA Security Rule 164.308(a)(8)). • Inform NCI of any subcontractors or other outside entities who will be given access to the caBIG™ systems (HIPAA Security Rule 164.308(b)(1)). • Implement security policies and procedures that limit physical access to facilities where the caBIG™ systems will be accessed (HIPAA Security Rule 164.310(a)(1)).
Management Office/Human Resources Or Institutional Equivalent	• Develop and assign roles and responsibilities for a Chief Security Officer (CSO) or equivalent that will be responsible for the implementation and enforcement of a comprehensive information security program consistent with the HIPAA Security Rule (HIPAA Security Rule 164.308(a)(2)). • Develop and implement administrative and oversight policies and procedures, including documentation of action taken, consistent with the HIPAA Security Rule.

6. Attachments

This SOP will be used in conjunction with the following attachments. These attachments must be used by all research sites conducting clinical trials under the caBIG™ Program and can be customized by individual research sites to accommodate format and content in accordance with local guidelines and/or requirements.

Title	Description
1) Procedure for HIPAA Security Requirements	This document provides the detailed steps to be followed in ensuring that access to the caBIG™ systems are in compliance with HIPAA Security Rule Requirements.