



**Title:** Agreement for Hosting Level 1 caGrid Services

**Status:** Final

**Version:** 1.0

**Effective Date:** 15 January 2008

**Sunset Date:** N/A

This Agreement for Hosting Level 1 caGrid Services (“Agreement”) is entered into by and between the National Cancer Institute (“NCI”), an agency of the United States Government, and \_\_\_\_\_ *<insert name of individual or institution>* (“NCI-caGrid Host”).

**Definitions:**

**caBIG™:** cancer Biomedical Informatics Grid.

**caGrid:** The underlying service-oriented infrastructure that supports caBIG™.

**NCI CBIT:** NCI Center for Biomedical Informatics and Information Technology.

**NCI-caGrid:** The instance of the caGrid infrastructure that is operated and maintained by the NCI, its contractors and subcontractors.

**caGrid Services:** Data services and analytical services that are caBIG™-compatible electronic information systems and can be registered by the NCI ca-Grid Host.

**Individual NCI-caGrid Host:** An individual who deploys a caGrid Service that connects to the NCI-caGrid by utilizing resources that are either provided by the Individual NCI-caGrid Host’s employer of record or are obtained independently.

**Institutional NCI-caGrid Host:** A legal entity whose employees or other authorized representatives deploy caGrid Services that connect to the NCI-caGrid by utilizing resources under the ownership or control of the institution.

**NCI-caGrid Host Signing Official:** The person that signs this Agreement on behalf of the NCI-caGrid Host. If the NCI-caGrid Host is an individual, that person is the NCI-caGrid Host Signing Official. The NCI-caGrid Host Signing Official is responsible for ensuring compliance with the terms of this Agreement.



**NCI-caGrid Operations Team:** NCI CBIIT approved personnel with access to the systems hosting the NCI-caGrid Level 2 Certificate Authority and who manage the operations and maintenance of the NCI-caGrid server.

**NCI-caGrid Certificate Authority:** An NCI CBIIT approved entity that issues digital certificates for NCI-caGrid authentication purposes in the form of a private key and certificate. The Certificate Authority should be trusted by reliant NCI-caGrid Level 2 parties.

**Purpose:** This Agreement describes the information security responsibilities of the NCI-caGrid Host with respect to connecting caGrid Services to the NCI-caGrid where, as described below, the hosted caGrid Services enable only non-sensitive data to be made available via the NCI-caGrid. The NCI-caGrid Host is responsible for compliance with any applicable provisions of local, state and federal statutes and regulations and this Agreement. Such applicable statutes and regulations include, but are not limited to:

1. Health Insurance Portability and Accountability Act of 1996 and implementing regulations as set forth in 45 CFR Parts 160, 162 and 164, as amended (hereafter HIPAA).
2. Basic HHS Policy for Protection of Human Research Subjects, as set forth in 45 CFR Part 46 as amended (known as the “Common Rule”).

Additionally, the NCI-caGrid Host is responsible for implementing policies and procedures at its site that enable compliance with the security principles described in this Agreement. NCI has adopted the following guidelines for establishment of authentication and risk assessment. The NCI-caGrid Host has assessed its security policies and procedures and asserts that they reasonably conform to the following standards or guidelines:

1. National Institute of Standards and Technology (NIST) Special Publication 800-63 (hereafter NIST 800-63)
2. Federal Information Processing Standards (FIPS) Publication 199 (hereafter FIPS 199)

Questions about this document should be directed to the Director of Quality Assurance and Compliance, NCI Center for Biomedical Informatics and Information Technology (CBIIT) at [ncicb@pop.nci.nih.gov](mailto:ncicb@pop.nci.nih.gov).

**Preliminary Conditions:** This Agreement may only be used by the NCI-caGrid Host to make *non-sensitive* information available through the NCI-caGrid. By accepting this Agreement, the NCI-caGrid Host agrees that:

1. It has evaluated the sensitivity of the data that it intends to make available through the caGrid Service(s) using either the FIPS 199 or a similar framework, and, based on that evaluation, has determined that the data are suitable for Level 1

credentials as described by NIST 800-63. These caGrid Services are known as Level 1 caGrid Services.

2. If necessary, it has obtained appropriate institutional approval in order to make the data presented by a Level 1 Grid Service available to a general audience without restriction.
3. It has complied with all appropriate institutional procedures for creating Level 1 caGrid Services.
4. The NCI-caGrid Host Signing Official has reviewed the current NCI-caGrid Security Policies (available at [https://gforge.nci.nih.gov/frs/?group\\_id=238&release\\_id=1044](https://gforge.nci.nih.gov/frs/?group_id=238&release_id=1044)) and agrees that it will comply with such policies while hosting any NCI caGrid Service(s).

**Responsibilities of NCI-caGrid Host:** By signing this Agreement, the NCI-caGrid Host agrees to accept the following responsibilities:

1. Compliance with Applicable Institutional Information Technology Policies and Procedures: For caGrid Services that are deployed by an Individual NCI-caGrid Host, to fully comply with all applicable institutional rules, policies and procedures for operation of information technology systems. The NCI-caGrid Host Signing Official asserts that s/he (a) is aware of such requirements, (b) has determined the tasks necessary to meet those requirements, and (c) has completed these tasks (including, but not limited to, any required institutional notifications).
2. Reporting: To report all security breaches or other security-related incidents by contacting NCI CBIIT Application Support at [ncicb@pop.nci.nih.gov](mailto:ncicb@pop.nci.nih.gov) or by telephone at 301-451-4384 or toll free at 1-888-478-4423, as soon as there is a reasonable basis for suspecting the breach. (Since the participants in NCI-caGrid utilize common enabling technologies, it is necessary that all security breaches be reported to the NCI-caGrid Operations Team by contacting the NCI CBIIT Application Support to maintain security.)
3. Participation in Security Investigations: To designate a point of contact and to update such designation to ensure currency at all times. This point of contact is responsible for transmitting information received from the NCI-caGrid Operations Team to the persons responsible for information security at the NCI-caGrid Host. The current NCI-caGrid designated contact is:  
\_\_\_\_\_ *<insert name, title, phone, email>*.
4. System Upgrades and Patches: To maintain the hardware and software supporting the Level 1 caGrid Service(s) by applying all publicly available security patches in a timely manner.

5. Data Confidentiality: To ensure that no Protected Health Information (as defined by HIPAA), data subject to regulation under the Common Rule or corresponding FDA regulations, data subject to special restrictions under state privacy laws, to the extent that they are more restrictive than HIPAA, or any other data that may be considered sensitive under applicable laws, regulations or institutional requirements, is made available through its Level 1 caGrid Service(s).
6. Resource Confidentiality: To maintain the security of the host certificates issued by NCI-caGrid Certificate Authorities and to immediately notify the NCI-caGrid Operations Team by contacting NCI CBIIT Application Support at [ncicb@pop.nci.nih.gov](mailto:ncicb@pop.nci.nih.gov), or by telephone at 301-451-4384 or toll free at 1-888-478-4423, if the private cryptographic keys have been compromised.

**Authority:** The NCI-caGrid Host is responsible for addressing any conflicts between the policies set forth in this Agreement and any other applicable nonfederal laws, regulations, policies or guidance. The NCI-caGrid Host represents that it has the authority to enter into this Agreement consistent with all employment, contractual and other obligations of the NCI-caGrid Host.

**Liability:** The NCI-caGrid Host understands that it is solely responsible for all activities under this Agreement and agrees that neither the NCI nor its contractors shall have any responsibility nor incur any liability for any of the NCI-caGrid Host's activities.

**Termination; Removal:** The NCI may, at its discretion, terminate this Agreement and revoke the credentials issued to the NCI-caGrid Host, thereby severing the connection with the NCI-caGrid of all caGrid services deployed by the NCI-caGrid Host upon violation of any of the terms of this Agreement. If the NCI-caGrid Host wishes to reinstate or to discontinue its provision of data under this Agreement, it will provide written notice to the NCI-caGrid Operations Team by contacting NCI CBIIT Application Support at [ncicb@pop.nci.nih.gov](mailto:ncicb@pop.nci.nih.gov).

**Signatures:**

Accepted by *<insert name of NCI-caGrid Host>*:

\_\_\_\_\_  
Name and Title of NCI-caGrid Host Signing Official

\_\_\_\_\_  
Date

Accepted by NCI CBIIT:

\_\_\_\_\_  
George A. Komatsoulis, Director QA and Compliance

\_\_\_\_\_  
Date