This System Interconnection and Hosting Security Agreement (System ISA) is entered into between the [specify] Cancer Registry (herein after referred to as “the registry”) and Information Management Services, Inc. having its principal place of business at 3901 Calverton Boulevard, Suite 200, Calverton, Maryland 20705 (herein after referred to as “IMS”).

**WHEREAS**, the registry has delegated authority for the purposes of collecting and reporting on population-based cancer incidence, treatment and survival data on all patients within the catchment area;

**WHEREAS**, IMS has the experience and capability to meet the specific information technology needs of the registry to fulfill its obligations.

**WHEREFORE**, the parties agree to the following:

# PURPOSE

The purpose of this System Interconnection and Hosting Security Agreement (System ISA) is to establish procedures between the registry and IMS regarding the development, management, operation, and security ofthe connections between registry staffand the registry’s data maintained in SEER\*DMS within IMS’s computer center. This System ISA is intended to ensure the confidentiality, integrity, and security of the registry’s data maintained within IMS’s computer center and while accessed by registry staff using the Internet.

The System ISA documents interconnection arrangements, registry and IMS commitments to data standards and integrity, and security responsibilities for the registry and IMS. This document specifies business requirements for the connection. The System ISA authorizes IMS to provide authorized registry staff with access to the registry’s data in SEER\*DMS and reiterates IMS’s commitment to protect the registry’s data from unauthorized access. For the purposes of this Agreement, IMS includes IMS employees, staff, and independent contractors, assignees and/or agents of IMS. IMS agrees to be bound to this Agreement and agrees to protect the confidentiality of Registry Data released to IMS by the Registry.

# SCOPE

* This System ISA applies to the registry data hosted by IMS.
* The System ISA applies to the information flows between the registry staff and the registry’s data maintained in SEER\*DMS within IMS’s computer center to support the registry’s production use of SEER\*DMS. The System ISA applies to all IMS and registry personnel involved in the working relationship.
* The registry and IMS applications and subnets that are not part of this system interconnection are not within the scope of this System ISA.

# SYSTEM DESCRIPTION

SEER\*DMS uses an HTML-based interface displayed via a web browser. Although the screens are displayed in a web browser, the system is not connected to the public internet. Access to the system requires a secure connection using a site-to-site virtual private network(s) (VPN) between the registry’s network and the SEER\*DMS server; or a client-to-site VPN configured on an individual workstation. The web-based design reduces maintenance of individual workstations by providing a mechanism for simultaneously delivering system upgrades to all registry desktops. No software, other than a web browser and possibly a VPN client, needs to be installed on the user’s computer.

The registry’s instance of the SEER\*DMS application and database will be hosted at an IMS computer center. Operations will be maintained using principles from National Institute of Standards and Technology’s (NIST) Risk Management Framework and controls will be maintained at the moderate level for each of confidentiality, integrity, and availability.

IMS’s VPN will be used to facilitate TLS and SFTP/SCP/SSH communications over the Internet to IMS for each registry staff member requiring access.

SEER\*Stat is an optional component. The VPN will only be configured for its protocol if the registry chooses to use it.

The registry and IMS will agree upon the most appropriate combination of site-to-site VPN(s) and client-to-site VPN technologies.

For client-to-site access, IMS’s secure sockets layer VPN (SSL-VPN) with digital certificates or the Google Authenticator will be used to facilitate communications over the Internet to IMS for each registry staff member requiring access. A separate digital certificate or smart phone configuration will be provided to each registry staff member requiring access. Each registry staff member’s full name and e-mail address will be required and maintained by IMS. The IMS VPN administrators will issue, maintain, and revoke these SSL-VPN credentials as necessary. Only appropriate staff authorized by the registry director shall create, maintain, modify, and delete the SEER\*DMS user accounts and roles unique to each registry staff member.

The VPN(s) will allow access to the IMS IP addresses associated with the registry’s SEER\*DMS services. The TLS protocol is necessary to access the Web based SEER\*DMS system. The SFTP/SCP/SSH protocol is necessary for SEER\*DMS auto-loading. The VPN(s) will not allow registry staff access to any IMS resources other than the IP address associated with registry’s SEER\*DMS services. Conversely, no IMS assets will be allowed any communications with registry information technology (IT) assets.

# BREACH AND SECURITY INCIDENT REPORTING

## Notification to the Registry

IMS shall notify the registry of any breaches or security incidents. IMS shall notify the registry’s IT Security Contact within 24 hours of IMS becoming aware of such breach or security incident.

## Report

IMS shall cooperate with the registry in investigating such breach or security incident, and in meeting the registry's obligations. IMS shall provide a written report to the registry within two business days of the breach or security incident. To the extent such information is available, the report must include, at a minimum: (i) the identification of each data element and individual whose information has been, or is reasonably believed to have been, accessed, acquired, or disclosed; (ii) the date of the breach or security incident; (iii) the scope of the breach or security incident; and (iv) a description of IMS's response or corrective action IMS took to mitigate the breach or security incident.

# COMMUNICATION AND IT SECURITY POINTS OF CONTACT

Mutual Responsibilities

Frequent formal communications are essential to ensure the successful management and operation of the relationship.

* The parties to this System ISA agree to maintain open lines of communication between designated staff at both the managerial and technical levels.
* In the event that any designated staff of either organization changes, the organization shall promptly inform the other of new designee’s contact information.

IMS Responsibilities

* Designate an IT security contact that shall act on behalf of IMS and communicate all IT security issues involving this connection agreement.
* The IMS designee shall be the IMS IT security official who shall be responsible for ensuring that the IT security controls for this connection meet the requirements of the registry.

# SERVICE LEVEL EXPECTATIONS

SEER\*DMS is expected to always be operational during the registry’s normal business hours.  Due to the nature of cancer registration and surveillance, planned downtime during non-business hours is acceptable as long as it does not rise to the level of negatively impacting the registry’s output.  Examples of events requiring planned downtime are software upgrades/patches, hardware replacement, operating system upgrades, etc.

IMS staff will work with registry managers to schedule maintenance windows. Routine server maintenance and upgrades will be conducted at regular intervals on a pre-defined schedule. These will typically be scheduled for one weekend morning each month. Additional maintenance windows may be necessary to mitigate an imminent problem or to apply a critical software patch. These will be scheduled with as much advance notice as possible and will be conducted at a time when system activity is at its lowest.

# OFF-SITE BACKUP AND DISASTER RECOVERY

IMS will back-up the registry’s data to a datacenter as least 50 miles away from the primary datacenter. This will be done in such a manner that no more than one day of data will be lost in the event of a disaster. Portable media will not be used for backup. Encrypted disks in the secondary datacenter, using the same technologies and type of infrastructure as the primary, will be used to store the off-site backups.

The secondary datacenter will have equivalent capabilities and physical security to the primary. IMS will maintain disaster preparedness consistent with being able to bring SEER\*DMS back up for operations in the secondary datacenter within 48 hours of an event.

Separate from the mechanisms described above, IMS will provide the option for each registry to self-host a third copy of their entire Postgres database. This will be for disaster recovery purposes in the unlikely event that both IMS datacenters are destroyed or compromised. The database will be packaged daily into a single tar.gz file which can be transferred to the registry on a scheduled basis. The tar.gz will be a Postgres file system level backup as described in Postgres documentation. It will require expertise in Linux and Postgres to make use of this file, but not expertise in SEER\*DMS.

# RESPONSIBLE DESIGNEES

### [Specify] Cancer Registry

Name:

Title:

Address:

Work Phone:

E-Mail:

### Information Management Services, Inc.

Name: R. Scott Depuy

Title: Chief Technology Officer

Address: IMS, Inc.

 3901 Calverton Blvd, Suite 200

 Calverton, MD 20705

Work Phone: 301-680-9770

Mobile Phone: 240-447-6750

E-Mail: depuys@imsweb.com

Name of Supervisor: Andy Lake

Title of Supervisor: President

# COMMITMENT TO PROTECT SENSITIVE INFORMATION

Mutual Responsibilities

* Do not release, publish, or disclose information to unauthorized personnel, and protect such information in accordance with provisions of the following laws and any other pertinent laws and regulations governing the adequate safeguard of agency information:
* 18 U.S.C. 1905 (Criminal Code: Disclosure of Confidential Information)
* Privacy Act of 1974 (5 U.S.C. § 552a)
* Ensure that any connection has a level of security that is commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information.

IMS Responsibilities

* Ensure that each employee and other authorized user with access to the registry’s data sign a non-disclosure agreement (NDA) or confidentiality pledge.
* Ensure that IMS use of registry data is only for these purposes:
	+ To investigate technical support issues submitted by registry staff.
	+ To test algorithms developed by IMS staff for the benefit of the registry.
	+ To test algorithms developed by external organizations for the benefit of the registry. The testing must be performed within the IMS computing facilities.
* Ensure that IMS will not release the data to external organizations with the exception of an external geocoding system. Registry data will be sent using a secure API to the Automated Geospatial Geocoding Interface Environment (AGGIE) developed through the partnership of NAACCR, NCI, and Texas A&M.

# COMMITMENT TO DATA STANDARDS AND INTEGRITY

IMS commits to providing system updates and related services in a timely manner; and to ensuring that SEER\*DMS processes completely and accurately support the registry’s mission for collecting and reporting population-based cancer surveillance data. IMS understands that registry data reporting must adhere to standards and requirements defined by local, state, and national standard setters. The national data setters include the North American Association of Central Cancer Registries (NAACCR), the National Cancer Institute’s SEER program, and the National Program of Cancer Registries (NPCR).

Registry Responsibilities

* Review and understand local, state, and national data standards and reporting requirements.
* Implement procedures and processes to ensure that registry staff are informed of changes to local, state, and national data standards and reporting requirements.
* Inform IMS of changes to local and state data standards in a timely manner.

IMS Responsibilities

* Ensure that SEER\*DMS data items adhere to data standards defined by local, state, and national standard setters.
* Ensure that edit sets provided by national standard setters are deployed in SEER\*DMS within two weeks of release. Provide support and system functionality to implement edits required to enforce local and state data standards.
* Implement functionality to create data extracts that conform to the reporting requirements of national standard setters. Provide support and system functionality to create data extracts that conform to the reporting requirements of local and state standard setters.

# DATA OWNERSHIP

IMS understands and reiterates here that the data subject to this agreement are the sole property of the registry. If the registry wishes to cease using SEER\*DMS, IMS will work in good faith to return the data to the registry, or work with the registry to transfer the data to another provider.

#

# FORCE MAJEURE

IMS’s failure to comply with any term or condition of this System ISA as a result of conditions beyond its fault, negligence, or reasonable control (such as, but not limited to, war, strikes, floods, governmental restrictions, riots, fire, other natural disasters or similar causes beyond IMS control) shall not be deemed a breach of this System ISA.

# SUCCESSOR

Notwithstanding anything stated in this Agreement to the contrary, any and all right, title and interest of the registry in and to the terms and conditions in this Agreement automatically transfer to the registry’s successor-in-interest by operation of law.   The transfer shall occur without further action and/or consent of the parties to the Agreement.

# LIABILITY

To the full extent allowed by law, each party hereto agrees to be responsible and to assume liability for its own wrongful or negligent acts or omissions, or those of its officers, agents or employees in its performance under this agreement. Each party agrees to assume responsibility for any and all claims, demands, actions, settlements or judgments involving either intentional or unintentional conduct, other than intentional malicious criminal wrongdoings, based upon or arising out of the activities described in this Agreement, to the extent that such claims, demands, actions, settlements or judgments are occasioned by the sole negligence, actions or omissions of each party, its trustees, faculty, students or employees.

*[Signature Page follows]*

**SIGNATURES**

Both parties agree to work together to ensure the joint security of the connection and the associated data stored, processed, and transmitted, as specified in this System ISA. Each party certifies that its respective system is designed, managed, and operated in compliance with all relevant federal and state laws, regulations, and policies.

We agree to the terms and conditions of this System ISA.

**[Specify] Cancer Registry**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

(Name)

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

(Title)

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

(Signature) (Date)

**Information Management Services, Inc.**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

(Name)

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

(Title)

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

(Signature) (Date)