DocuSign Envelope ID: 9C66829C-D27D-4C56-AF5E-45423BAE2FAA

SEER*DMS SYSTEM INTERCONNECTION SECURITY AND HOSTING AGREEMENT BETWEEN THE TEXAS DEPARTMENT OF STATE HEALTH SERVICES AND INFORMATION MANAGEMENT SERVICES, INC.

This System Interconnection and Hosting Security Agreement (System ISA) is entered into between the Texas Department of State Health Services on behalf of the Texas 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. IMS was selected by the National Cancer Institute Surveillance, Epidemiology, and End Results (SEER) program to provide these information technology services for the SEER registries.

WHEREAS, IMS develops, maintains, and hosts a data management system for SEER registries (SEER*DMS); and

WHEREAS, the Registry has been awarded a contract with the National Cancer Institute (NCI) SEER Program to participate as a SEER registry and, pursuant to the contract, the Registry is required to use IMS' SEER*DMS and hosting services.

WHEREFORE, the parties agree to the following:

1 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 of the connections between registry staff and the registry's data maintained in SEER*DMS within IMS's computer center. This agreement falls within the expectations of the registry's SEER contract No. 75N91021D00011 with NCI. This System ISA is intended to ensure the confidentiality 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 and security responsibilities for the registry and IMS, and 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.

DocuSign Envelope ID: 9C66829C-D27D-4C56-AF5E-45423BAE2FAA

2 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.

3 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 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. The registry's data stored on IMS servers, or "islands" will be secured in accordance with the requirements specified in the registry's SEER contract No. 75N91021D00011 with NCI. 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/SSL, SFTP/SCP/SSH, Postgres, and SEER*Stat 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 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 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/SSL protocol is necessary to access the Web based SEER*DMS system. The

DocuSign Envelope ID: 9C66829C-D27D-4C56-AF5E-45423BAE2FAA

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 IT assets.

3.1 JOINTLY OWNED ISLAND

SEER is working with a variety of health care industry organizations to obtain more data streams to enhance the registry data. These data include, but are not limited to, pharmacy data, claims data, radiation information, genetic information, etc. Many of these organizations function in multiple states, and hence have data related to multiple registries.

IMS, as the technical and IT support provider for the registry, will work with the health care industry organizations to provide a single point where the data will be received. This will be a server, or "island", that is jointly owned by all SEER*DMS registries. While IMS will host and maintain this island, data on this island will not be owned by IMS. The purpose of this island is to provide the single communication point for the data streams, to split the data stream by geographic region, and to pass the resulting region-specific data to the relevant cancer registry. IMS will not retain the data after it has been passed to the appropriate registry, nor will IMS retain any data falling outside any region of interest. The joint island may also be used to transfer data back to the health care industry organization if required by the project and upon approval by the registry.

This agreement gives IMS permission to work on the registry's behalf to host the jointly owned island, to develop logic to split the data stream, and to then pass that region specific data to the registry's SEER*DMS island. It also gives IMS permission to pass files approved by the registry back to the health care industry organization.

The health care industry organization will be able to move data to the jointly owned island, to receive files passed back by the registry, but will not be able to access that island in any other way. They will not have any access to any of the registry specific SEER*DMS islands.

The registry will be able to receive data from the jointly owned island, but will not be able to access that island in any other way. The registry will not have any access to the health care industry organization's networks.

The security controls and operational posture of the jointly owned island are equivalent to those for the registry specific SEER*DMS islands.

4 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.

DocuSign Envelope ID: 9C66829C-D27D-4C56-AF5E-45423BAE2FAA

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.

5 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.

6 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.

DocuSign Envelope ID: 9C66829C-D27D-4C56-AF5E-45423BAE2FAA

7 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.

8 COSTS

IMS's compensation for the continued development, maintenance, and configuration of the SEER*DMS software will be provided by a contract between IMS and The SEER Program, NCI. The parties to this agreement will convene annually to arrange for the hosting and related fee terms and conditions.

9 RESPONSIBLE DESIGNEES

Texas Department of State Health Services

Name:	Manda Hall
Title:	Associate Commissioner, Community Health Improvement
Address:	P.O. Box 149347 Austin, TX 78714
Work Phone:	512-776-7321
E-Mail:	Manda.Hall@dshs.texas.gov

Information Management Services, Inc.

Name:	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

DocuSign Envelope ID: 9C66829C-D27D-4C56-AF5E-45423BAE2FAA

10 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.
- Ensure that IMS will safeguard confidential information received from registry in compliance with the HHS Data Use Agreement, Attachment A, and the Security and Privacy Initial Inquiry, Attachment 2.

11 CONTRACT SUPPLEMENTAL CONDITIONS

- **Attachment A, HHS Data Use Agreement v.8.5 ("DUA")**, of this Contract is revised as follows. Unless expressly modified, amended, or replaced in this section, the original **DUA** contained in **Attachment A** shall remain in full force and effect:

  - ARTICLE V, GENERAL PROVISIONS, Section 5.07(A), Insurance, is deleted in its entirety and replaced with the following:

    Section 5.07 Insurance

DocuSign Envelope ID: 9C66829C-D27D-4C56-AF5E-45423BAE2FAA

(A) Contractor shall be responsible for reasonable expenses covered by, and up to the limit of, the Contractor's applicable insurance coverage, damages assessed upon Contractor as a result of the failure of the Contractor, its officers, directors, employees, Subcontractors or agents for failure to comply with this DUA or any requirement applicable to Contractor under HIPAA, as amended from time to time. Contractor will maintain an applicable insurance policy which covers network security and privacy-related liability with a coverage value of no less than $10,000,000. Notwithstanding any other provision of the Agreement or this DUA to the contrary, this Section shall survive the expiration or termination of this DUA for any reason.

All other provisions of HHS Data Use Agreement, version 8.5 dated October 23, 2019 with Security and Privacy Inquiry (collectively, DUA) shall remain in full force and effect. If there is any conflict between the terms of this Agreement and the terms of the DUA, the terms of the DUA shall take precedence.

12 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. If the registry ceases its participation in SEER but wishes to continue using SEER*DMS, IMS will provide the registry with an updated proposal to continue the hosting relationship.

13 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.

14 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.

DocuSign Envelope ID: 9C66829C-D27D-4C56-AF5E-45423BAE2FAA

15 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.

16 CONTRACT PERIOD

This agreement will be effective from May 1, 2021 or on the signature date of the latter of the Parties to sign this agreement through April 30, 2028.

DocuSign Envelope ID: 9C66829C-D27D-4C56-AF5E-45423BAE2FAA

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.

Texas Department of State Health Services

Manda Hall_____
(Name)

Associate Commissioner, Community Health Improvement_
(Title)

DocuSigned by:
Manda Hall, MD April 30, 2021
202CEA5A9C164E3...
(Signature) (Date)

Information Management Services, Inc.

_R. Scott Depuy_____
(Name)

_Chief Technology Officer_____
(Title)

5/3/2021
(Signature) (Date)