DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Information Security Agreement
PAGE: 1 of 5	**REPLACES POLICY DATED:** 2/15/10, 5/15/10, 12/1/10, 9/1/11, 12/1/14, 1/1/18, 9/1/20, 8/1/21
EFFECTIVE DATE: September 1, 2023	**REFERENCE NUMBER:** IP.SEC.008 (formerly IS.SEC.008)
APPROVED BY: Ethics and Compliance Policy Committee	

SCOPE:

This policy applies to all HCA Healthcare affiliates, including facilities, Divisions, Company business units and all Corporate Departments.

PURPOSE:

This policy sets forth the requirements for Information Security Agreements (each an "ISA"), which are designed to standardize protection of the Company against security risks presented by all Counterparties that have access to the Company Network, Infrastructure, and/or Data. In addition to standardizing protection against security risks, ISAs also help ensure ownership of Data and contractual protection against breaches or misuse of Data caused by Counterparties with access to Data. Except as expressly provided in Section 5 (*Exceptions*) of this policy, all Counterparties that have access to the Company Network, Infrastructure, and/or Data are subject to this policy. This policy does not apply to information that is publicly available, nor does it apply to internal access among Company workforce members and/or Company entities.

POLICY:

1. This policy applies to all Counterparties, each of which are required to sign an ISA, prior to being permitted to (a) connect to, and/or have access to Network or Infrastructure, or (b) store, process, transmit, or otherwise be permitted any access to Data. The ISA requires certain security controls to be in place in order to protect Network, Infrastructure, and/or Data. Any exceptions to the ISA requirements will be determined by designated Information Protection & Security ("IPS") personnel, and/or in accordance with applicable Policy (e.g., the Information Security Risk Acceptance and Accountability Policy, IP.SEC.009). ISAs are required in addition to any other agreements, whether required by law, Company policy, or otherwise (e.g., Governing Agreements, Business Associate Agreements, Data Protection Agreements, Data Use Agreements, External Data Release approval, Third Party Application approval process, etc.). This policy applies to new requests and renewals of existing contracts occurring on or after the effective date that include the requirement of an ISA.
2. When Governing Agreements are renewed, IPS may require execution of an updated ISA.
3. Any suggested revisions to the ISA by Counterparties must be reviewed and approved by:
    a. HCA Healthcare Technology Law Group (or delegated outside counsel); and
    b. For Corporate departments, and US Divisions, designated IPS personnel; or, for the UK Division, the Information Governance & Security group.
4. The ISA must be signed by both parties before (a) any services, purchasing, managed care, participation, or other agreement and/or ordering document may be signed, (b) any Products

or Services are paid for, (c) any Products and/or Services are provided to the Company, and (d) any Data is provided to or otherwise accessible by the Counterparty.

5. **Exceptions**. The following are excepted from this Policy:
   a. Oral communications or limited sharing of individual Data elements in the ordinary course of business;
   b. Accreditation organizations *(*e.g., The Joint Commission, American College of Surgeons, Society of Thoracic Surgeons, Society of Cardiovascular Patient Care, College of American Pathologists, American Academy of Sleep Medicine, Accreditation Council for Graduate Medical Education), unless as otherwise required (or deemed necessary) by IPS leadership;
   c. Registries (e.g., Cancer Registry, Death Registry, Medical Device Registries);
   d. Government reporting requirements (e.g., federal, state);
   e. Healthcare providers (e.g., non-employed physicians) who are accessing Data to provide patient care to the Company's patients. For clarity, this exception does not apply when a healthcare provider also provides Products and/or Services beyond or in addition to direct patient care that result in access to the Company Network, Infrastructure, and/or Data;
   f. Covered Entities and their Business Associates to the extent that access to Network, Infrastructure, and/or Data is limited solely to claims reimbursement. For purposes of clarification, Covered Entities and/or their Business Associates with access to Network, Infrastructure, and/or Data for any reason other than claims reimbursement will not be exempt from this policy;
   g. For the UK Division, governmental embassies to the extent that such governmental embassies' access to Data is limited solely to patient referrals and payment for hospital and provider services; and
   h. Parties receiving Data pursuant to a HIPAA-compliant authorization.

PROCEDURES:

1. **Enterprise ISAs.** Corporate ITG Contracts Department and designated IPS personnel process and maintain all enterprise ISAs.
   a. **Alternative ISAs.** All ISAs should be negotiated and executed as Enterprise ISAs in accordance with Section 1 immediately above, unless designated IPS personnel have approved execution of an alternative agreement.
   b. For ISAs submitted by Divisions (US or UK) or facilities, any changes to Attachment B (technical terms) must be reviewed and, as applicable, negotiated by designated IPS

personnel and the ITG UK Information Governance group at the UK Division level. Any change to Attachment A (legal terms) or Attachment C (definitions) must be reviewed and finalized by HCA Healthcare Technology Law Group (or delegated outside counsel) before the ISA may be signed.

2. **Payer ISAs.** Corporate ITG Contracts Department and designated IPS personnel process and maintain all Payer ISAs, regardless of whether the Payer ISA is enterprise, Division (US), or facility level.

3. **Required Roles.** The following roles must be involved in the ISA negotiation process:
   a. Designated IPS personnel for US ISAs;
   b. The Information Governance & Security group for UK Division ISAs;
   c. HCA Healthcare Technology Law Group (or delegated outside counsel);
   d. HCA Healthcare Payer Contracting and Alignment Legal Counsel for approval of the Payer ISA requests.

4. **Additional Roles.** The following roles should be notified and consulted, as applicable, during the ISA negotiation:
   a. Named business owner(s) or sponsor(s) impacted by purchase of vendor product or service or relationship with Counterparty, if applicable; and
   b. Facility, Division, or Corporate executives, as needed.

5. **Authorized Signatory.** The ISA must be signed by authorized signatories for each of the parties entering into the ISA.

6. **Precedence of Agreements/ Conflicts Provision Required in the Governing Agreement.** The terms of any Governing Agreement where an ISA is also required should provide a conflicts provision with respect to data security and confidentiality that gives precedence to whichever agreement is more protective of Company.

7. **Accompanying Statement of Work (SOW).** With the exception of Payer ISAs, the ISA negotiation process should not be initiated unless the business owner and/or sponsor is contemporaneously pursuing a statement of work or other purchasing document.

8. **Legal Entities.** The ISA must reflect the name of the actual legal entities that are entering into the contract. In most cases, these will be the same legal name that signed the Governing Agreement.

HCA Healthcare

DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Information Security Agreement
PAGE: 4 of 5	**REPLACES POLICY DATED:** 2/15/10, 5/15/10, 12/1/10, 9/1/11, 12/1/14, 1/1/18, 9/1/20, 8/1/21
EFFECTIVE DATE: September 1, 2023	**REFERENCE NUMBER:** IP.SEC.008 (formerly IS.SEC.008)
APPROVED BY: Ethics and Compliance Policy Committee	

DEFINITIONS:

Counterparty means any party that has access to the Network, Infrastructure, and/or Data of the Company and/or its Affiliates. Examples of Counterparties include, but are not limited to payers, such as managed care organizations or indemnity insurers, research partners, and all suppliers, including direct vendors, value-added resellers, and vendors indirectly providing products or services through value-added resellers.

Data means (a) all data and information the Company and/or its Affiliates provide to a party, made accessible by the Company and/or its Affiliates to a party, or to which a party has access or that a party (or such party's Products or Services) retrieves or collects during the course of performance of a Governing Agreement; (b) all archives, derivatives, summaries, abstracts, compilations, combinations with other information, modifications or manipulations of the foregoing data or information, aggregated information, de-identified information, data sets, subsets, and the like related to, or derived from such data or information; and (c) all reports generated by the Products and Services, or otherwise generated or provided by a third party relating to or in connection with the Product or Services.

Infrastructure means any information technology system, virtual or physical that the Company or its Affiliates own, control, lease, or rent, and that resides on or outside the Network. ITG Infrastructure obtained from an IaaS (Infrastructure as a Service), PaaS (Platform as a Service), or SaaS (Software as a Service) provider will be located on the ITG Network as part of a Service.

ISA means an Information Security Agreement.

Governing Agreement means any agreement between a Counterparty and the Company and/or any of its Affiliates for the purchase, lease, licensing, and acquisition or servicing of a Product or provision of Services, regardless of whether the Company has any payment obligations under the agreement.

Network means any non-public Wide Area Network (WAN) or Local Area Network (LAN) owned, operated, managed or controlled by the Company or its Affiliates.

Payer ISA means an information security agreement or exhibit to a Data Access or other Managed Care Agreement entered into with a managed care organization, indemnity insurer, or a related service provider, pursuant to payer contracting and alignment activities.

Product means any software, hardware, operating system, computer equipment or product provided by a Counterparty to the Company and/or its Affiliates, including, without limitation, any new version, replacement version, patch, error correction, new release, or security patches.

DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Information Security Agreement
PAGE: 5 of 5	**REPLACES POLICY DATED:** 2/15/10, 5/15/10, 12/1/10, 9/1/11, 12/1/14, 1/1/18, 9/1/20, 8/1/21
EFFECTIVE DATE: September 1, 2023	**REFERENCE NUMBER:** IP.SEC.008 (formerly IS.SEC.008)
APPROVED BY: Ethics and Compliance Policy Committee	

Service means any service provided by a Counterparty (or its contractor, independent contractor, officer, director, employee, consultant or other representative of such party, whether under oral or written agreement, whether an individual or entity as well as any application, tool, script, process or other similar application used by such party or any of the foregoing) to the Company and/or its Affiliates, including but not limited to, SaaS (Software as a Service), maintenance and support service, program development service, consulting service, outsourcing service, hotline or telephone assistance, or other professional service.

REFERENCES:

1. Information Security Agreement – Atlas Connect site
2. Information Security Risk Acceptance and Accountability Policy, IP.SEC.009
3. Information Protection – Release of Company Data to External Entities, IP.GEN.004
4. ITG Contracts Atlas Connect page
5. Business Associate Agreement Atlas Connect page
6. ITG Finance & Administration Atlas Connect page