DEPARTMENT: Information Protection & Security	**POLICY DESCRIPTION:** Release of Company Data to External Entities
PAGE: 1 of 7	**REPLACES POLICY DATED:** 1/2/18, 1/3/18, 9/1/19
EFFECTIVE DATE: December 1, 2021	**REFERENCE NUMBER:** IP.GEN.004
APPROVED BY: Ethics and Compliance Policy Committee	

SCOPE: All Company-affiliated facilities and Lines of Business including, but not limited to, hospitals, ambulatory surgery centers, home health agencies, hospice agencies, imaging and oncology centers, physician practices, shared services centers, corporate departments, Groups, Divisions and Markets (collectively with HCA Healthcare, the "Company").

EXCLUSIONS:

1. The Policy is limited to *external* releases of Company Data, and does not apply to *internal* Data-sharing among HCA Healthcare colleagues and entities or information that is publicly available.
2. The Policy does not apply to oral communications or limited sharing of individual pieces of Company Data in the ordinary course of business.
3. Any external release of Protected Health Information (PHI) to Covered Entities for Treatment, Payment, and Limited Health Care Operations as defined under HIPAA are excluded from the requirements of this Policy.
4. Certain external releases of PHI as defined under HIPAA as disclosures which require a HIPAA-compliant authorization, disclosures to entities other than Covered Entities which are permissible *without* the patient's authorization or *without* the patient's agreement or objection are excluded from the requirements of this Policy provided they meet the requirements of the Procedure section below.
5. The Policy does not apply to external releases of Company Data that are supervised by HCA Healthcare's corporate legal counsel or other approved corporate processes and that are either: (1) protected under client-attorney privilege, (2) related to litigation, insurance or indemnity claims, or similar risk management activities, (3) required as part of an acquisition, divestiture or investment transaction process, (4) supervised due diligence, fair market valuation assessments or similar research, (5) responsive to a subpoena or other similar government investigation power, or (6) otherwise required by law.
6. The Policy does not apply to external releases of Company Data to auditors or accounting consultants properly engaged in the ordinary course of the Company's financial audit and tax engagements.
7. The Policy does not apply to agreements which existed prior to the original effective date of this Policy; it only applies to *new requests* and *renewals of existing contracts* that include the release of Company Data to External Entities.
8. This Policy does not apply to external releases of PHI required under the 21st Century Cures Act and its implementing regulations prohibiting information blocking (commonly known as the "Information Blocking Rules" and codified at 45 CFR Part 171) as described in the Information Blocking Rule Compliance Policy, IP.GEN.006 provided they meet the requirements of the Procedure Section 14 below.

BACKGROUND: The Company's policies for management of Confidential Information require all colleagues with access to such information to obtain appropriate permissions before sharing

DEPARTMENT: Information Protection & Security	**POLICY DESCRIPTION:** Release of Company Data to External Entities
PAGE: 2 of 7	**REPLACES POLICY DATED:** 1/2/18, 1/3/18, 9/1/19
EFFECTIVE DATE: December 1, 2021	**REFERENCE NUMBER:** IP.GEN.004
APPROVED BY: Ethics and Compliance Policy Committee	

Confidential Information, and this policy is designed to provide an efficient procedure for obtaining that approval for Company Data releases.

Company-affiliated facilities collect information from patients, workforce members, practitioners, and third parties; generate data through clinical, research, and management services; and exchange data with third parties in normal operations. The location and custody of Company Data is broadly distributed across the Company, and the Company's colleagues have broad system access with the ability to collect, extract, compile and distribute data in spreadsheets, electronic format, written reports, etc. and the external demand to share data is increasing rapidly.

In addition to traditional confidentiality concerns, Company Data has significant and growing patient care, research, and business value that must be protected in the interest of both our patients and the Company. External Entities in research, consulting, and commercial relationships with Company-affiliated facilities may seek access to Company Data and even submit contract terms and procedures related to ownership or rights to use Company Data that do not represent appropriate use of this data.

This Policy establishes a framework for review of requests for sharing Company Data with External Entities including risk assessment, legal engagement, and approval procedures for protecting Company Data.

Note: Capitalized terms used in this Policy are defined in Appendix A: Definitions.

POLICY:

1. Company-affiliated colleagues must obtain approval through the procedures set forth in this Policy prior to releasing Company Data to External Entities.
2. Requests to release Company Data to External Entities must be reviewed by an appropriate Responsible Attorney, Responsible Officer and/or the HCA Healthcare Value Management Committee (VMC).
3. Responsible Attorneys must confirm agreements are in place containing language governing use of Company Data in accordance with the Request.
4. Responsible Attorneys must document decisions to: (1) deny, or (2) approve (with or without modifications) the Request.
5. Responsible Officers must document decisions to: (1) deny, (2) approve (with or without modifications), or (3) escalate each request to a Senior Responsible Officer or the VMC.
6. Sponsors of requests to release Company Data to External Entities must ensure the Data released to External Entities contains only Data Sets approved by the Responsible Officer and/or the VMC.
7. Sponsors may submit requests to establish Direct Access to the Company network or provide Continuous Data to External Entities only after VMC approval and execution of appropriate contractual documents.

DEPARTMENT: Information Protection & Security	**POLICY DESCRIPTION:** Release of Company Data to External Entities
PAGE: 3 of 7	**REPLACES POLICY DATED:** 1/2/18, 1/3/18, 9/1/19
EFFECTIVE DATE: December 1, 2021	**REFERENCE NUMBER:** IP.GEN.004
APPROVED BY: Ethics and Compliance Policy Committee	

8. Sponsors must remove an External Entity's access to Company Data in a timely manner upon termination of the relationship, contract, etc.
9. HCA Healthcare Information Protection & Security (IPS), in coordination with the VMC, HCA Healthcare Legal Department, and other subject matter experts, shall provide training and resources to facilitate implementation of this Policy.

Note: Approval of a request to release Company Data to an External Entity does not remove requirements for contracting components such as a Business Associate Agreement (BAA), Data Use Agreement (DUA), or Information Security Agreement (ISA).

PROCEDURE:

1. A colleague of a Company-affiliated facility ("Sponsor") with a business requirement to share Company Data with an External Entity starts the approval process by submitting a Request to Release Company Data to an External Entity ("Request") through the IPS process that includes use of the External Data Release (EDR) Tool.

2. IPS will review and confirm the accuracy of the request and will either (1) route the Request to the appropriate Responsible Officer based upon the categorization of the data release or (2) send back to the Requestor for edits or cancellation.

3. A Responsible Officer may approve a Request from their organization if it is a Single or Recurring Data Set being released for Restricted Use.

4. The following Requests require escalation for VMC approval:
   a. Contracts that do not restrict use of the data (i.e., Unrestricted Use)
   b. Continuous Data release (aka "streaming" data flow), whether Restricted Use or Unrestricted Use
   c. Direct Access to the Company network and/or its information systems

5. The VMC may approve a Request from any part of the organization and for any category of use.

6. Upon approval of a Request by the Responsible Officer or VMC, the Sponsor shall ensure Data released to the External Entity is protected in accordance with applicable federal, state and/or local regulatory provisions and Company IPS policies and standards, and contains only the Data Sets approved by the Responsible Officer or VMC.

7. Sponsor of an External Entity approved by the VMC for Direct Access to the Company network and/or its information systems must use the electronic Security Access Form (eSAF) tool to: (1) document approval for provisioning access for the External Entity's Representatives; and (2) trigger notification to Information Technology Group (ITG) system administrators to provision access (e.g., create network logon IDs).

8. Sponsor must also use eSAF to trigger removal of Direct Access by the External Entity's Representatives within one business day based upon the effective date of: (1) termination of the External Entity's contract; or (2) revocation of approval for the External Entity's representatives having Direct Access; or (3) External Entity's notification about termination of a representative.

   Note: Any individuals granted Direct Access (based upon authoritative classification as one of the following types of service providers) are still subject to the Policy requirements with respect to their use of Company Data, but their Direct Access to Company Data ***solely*** on their capacity as a service provider does not require submission via the EDR Tool because their individual access is instead captured using eSAF approval workflows.
   a. Licensed Independent Practitioner (LIP)
   b. Advanced Practice Professional (APP)
   c. Contractor (assigned responsibilities comparable to a colleague)
   d. Physician Office Staff/Support
   e. Dependent Healthcare Professional (DHP)
   f. Network/Per Diem Personnel
   g. Traveler
   h. Resident/Fellow (Medical)
   i. Student (Medical)
   j. Student (Nursing)
   k. Student/Intern
   l. Faculty/Instructor (clinical)
   m. Volunteer
   n. Federal/State/Government Surveyor

9. Corporate Department(s) who release Company Data to the External Entity types listed below on behalf of one or more HCA Healthcare facilities have a standing approval by the VMC for release but must maintain an inventory of such releases for inclusion in the EDR Tool. For any releases to the External Entity types listed below that are not in compliance with the first sentence in this Section 9, a Sponsor must submit a "Request for Release of Company Data".
   a. 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)
   b. Registries (e.g., Cancer Registry, Death Registry, Medical Device Registries)
   c. Federal and State Reporting

10. Releases of PHI to an External Entity that is a Covered Entity which are permissible under HIPAA are *excluded* from the requirements of this Policy when the release is related to Treatment, Payment and Limited Health Care Operations, all as defined by HIPAA. This exemption includes:
    a. PHI accessed, used or disclosed to another health care provider which meets the definition of a Covered Entity, as defined by HIPAA, for the receiving provider's Treatment activities

such as the continuum of care when a shared patient relationship exists between the two health care providers.

b. PHI accessed, used or disclosed to a health plan which meets the definition of a Covered Entity, as defined by HIPAA, for the receiving provider's Payment activities such as verifying eligibility or billing when a shared patient relationship exists between the provider and the health plan.
c. PHI accessed, used or disclosed to another Covered Entity (e.g., another hospital, physician, health plan), for the receiving Covered Entity's case management, quality assessment, training and education, accreditation, certification, licensing, or protocol development activities when a shared patient relationship exists between the two Covered Entities.

11. Releases of PHI to an External Entity other than a Covered Entity as needed to comply with an Approved Purpose (as set forth below) that are permissible without the patient's authorization or without the patient's agreement or objection are *excluded* from the requirements of this Policy all as defined by HIPAA.
    a. This exemption only applies to PHI that is disclosed for one of the following "Approved Purposes":
        i. Public Health Activities
        ii. Health Oversight Activities
        iii. Decedents
        iv. Reviews Preparatory to Research
        v. Disclosures to Avert a Serious Threat to Health or Safety
        vi. Disclosures for Specialized Government Functions
        vii. Disclosures for Workers' Compensation
        viii. Research disclosures of EHI (which is a subset of PHI and defined in the Information Blocking Rule Compliance Policy) pursuant to an IRB Waiver of Authorization/Consent (see Procedure 14 below).
    b. This exemption DOES NOT include (and thus this policy DOES apply to):
        i. Research disclosures of PHI that do not fall under Procedure Section 14 below pursuant to an IRB Waiver of Authorization/Consent;
        ii. Disclosures of de-identified information for clinical research use (e.g. into a research data repository or pursuant to a journal's research data sharing requirements).

12. Releases of Company Data to an External Entity that are supervised by the Company's corporate legal counsel, financial audit personnel or tax management personnel are excluded from the requirements of this Policy when the release is subject to the attorney-client privilege or subject to an engagement letter, business associate agreement or similar agreement that provides for Restricted Use and confidential treatment of Company Data. This exemption includes:
    a. Releases related to litigation, insurance or indemnity claims or similar risk management activities;
    b. Releases related to risk assessments or management by legal counsel;
    c. Releases that are required as part of an acquisition, divestiture or investment transaction

process;
   d. Releases as part of supervised due diligence, fair market valuation assessments or similar research supervised by the legal department;
   e. Releases that respond to a subpoena or other government investigation;
   f. Releases that are required by law;
   g. Releases related to the Company's financial audit activities; and
   h. Releases related to the Company's tax management and audit functions.

13. To the extent that a Release of Data to an External Entity includes Data that is subject to or otherwise governed by separate contract (i.e., not the contract that governs the Release itself which is the current subject to review under this Policy, but a separate contract of the Company related to governance or use of Data in this Release), nothing in this Policy shall be deemed to:
    a. Supersede that contract or authorize any Release or use that is not in compliance with the terms of such contract.
    b. Limit the ability of the Company to handle Data belonging to third parties or provide services related to third party Data pursuant to the terms of an existing agreement with such third party, including Release of such party's data to that party directly (with or without modification), whether aggregated, manipulated, modeled for expected performance, or otherwise in compliance with the terms of such agreement.

14. To the extent a Release of PHI to an External Entity involves PHI that meets the definition of EHI as set forth in the Information Blocking Rule Compliance Policy, IP.GEN.006, the request should be reviewed to determine whether disclosure is required by the Information Blocking Rule Compliance Policy. If disclosure is required by the Information Blocking Rule Compliance Policy, this Policy does not apply.

REFERENCES:

1. AC.UAM.01, ISAM Procedures Standard
2. AC.UAM.02, User Access Authorization, Establishment, and Modification Standard
3. COG.PPA.002, Licensure and Certification - Implementation Tools
4. COG.PPA.003, (DHP Policy) Implementation Tools
5. HR.ER.002, Background Investigation Attestation
6. IP.PRI.001, Patient Privacy Program Requirements
7. IP.PRI.010, Authorization for Uses and Disclosures of Protected Health Information
8. IP.PRI.012, Safeguarding Protected Health Information
9. IP.PRI.013, Mitigating Inappropriate or Unauthorized Access, Use and/or Disclosure of Protected Health Information
10. Privacy Model Policy - Limited Data Set and Data Use Agreements
11. Privacy Model Policy - Determination, Uses and Disclosures of De-identified Information
12. Privacy Model Policy - Uses and Disclosures for which an Authorization or Opportunity to Agree or Object is Not Required

DEPARTMENT: Information Protection & Security	**POLICY DESCRIPTION:** Release of Company Data to External Entities
PAGE: 7 of 7	**REPLACES POLICY DATED:** 1/2/18, 1/3/18, 9/1/19
EFFECTIVE DATE: December 1, 2021	**REFERENCE NUMBER:** IP.GEN.004
APPROVED BY: Ethics and Compliance Policy Committee	

13. Privacy Model Policy - Uses and Disclosures of PHI to Other Covered Entities and Health Care Providers
14. Privacy Model Policy - Uses and Disclosures Required by Law Policy
15. IP.GEN.002, Protecting & Mitigating Inappropriate or Unauthorized Access, Use and-or Disclosure of Personally-Identifiable Info
16. IP.GEN.006, Information Blocking Rule Compliance
17. IP.SEC.005, Information Confidentiality and Security Agreements Policy
18. IP.SEC.008, Information Security Agreement
19. Information Protection - Electronic Data Classification Standard
20. Information Protection Model Procedure - Access Authorization
21. Information Protection Model Procedure - Authorization and Supervision
22. WS.TCE.01, Termination Notification
23. COG – Clinical Research Support

HCA Healthcare

APPENDIX A: DEFINITIONS

Access is the ability of an External Entity to view, record, manipulate, download or otherwise access or use Company Data, whether (a) in hard copy (via report, presentation or otherwise), (b) by delivery of Data in electronic form, file or stream, or (c) through Direct Access to Company information systems.

Approval means, with respect to any request for Access to Data, the approval prescribed in this Policy based on the specific aspects of such request for Access.

Approved Terms means, with respect to any contract that includes Access to Data, the standardized terms regarding Data access, use and management that are included in the form agreement and approved by the Company's General Counsel or assigned delegate.

Company includes all Company-affiliated facilities and Lines of Business including, but not limited to, hospitals, ambulatory surgery centers, imaging and oncology centers, physician practices, shared services centers, corporate departments, Groups, Divisions and Markets (collectively with HCA Healthcare, the "Company").

Company Data is any and all Confidential Information generated, obtained or held by the Company in the course of its operations (whether text, images, code, graphics, video or other information) in any form, and however stored, transmitted or generated, including, without limitation all archives, derivatives, modifications or manipulations of the foregoing information.

Confidential Information is information which is not publicly known, including, but not limited to: information about patients' health or demographics, health insurance claim numbers, financial information, marketing information, company human resources, payroll, business plans, projections, sales figures, pricing information, budgets, credit card or other financial account numbers, customer and supplier identities and characteristics, plans, sponsored research, processes, schematics, formulas, trade secrets, innovations, discoveries, data, dictionaries, models, organizational structure and operations information, strategies, forecasts, analyses, credentialing information, Social Security numbers, passwords, PINs, and encryption keys. Confidential Information does not include information that: (i) was publicly known through no wrongful act; (ii) was in lawful possession prior to disclosure and was not received as a breach of any confidentiality obligations; (iii) was independently developed; or (iv) was lawfully obtained from a third party without confidentiality restrictions.

Continuous Data is provided to the External Entity on a continuous or steady basis, but for which the delivery does not qualify as a Recurring Set.

Covered Entity A health plan (e.g., an individual or group plan that provides or pays the cost of medical care), a health care clearinghouse, or a health care provider who transmits any health information in connection with a transaction covered by the Health Insurance Portability and Accountability Act (HIPAA).

Data Set is a collection of related items of Data that is composed of separate elements, but can be manipulated as a unit, such as the contents or output of the Company's Enterprise Data Warehouse, or database information of any type.

Direct Access is when an External Entity and/or its Representatives (e.g., colleagues, contractors) are granted the technical ability to connect to the Company network and/or its

information systems. This approach enables the External Entity and/or its representatives to independently view, record, manipulate, download or otherwise access or use Company Data.

Electronic Security Access Form (eSAF) is the Company-wide workflow tool used to maintain electronic audit evidence about business decisions to provide access to information stored or maintained in Company information systems.

Executive Governance Committee (EGC) provides oversight for the VMC and includes the Company's Chief Operating Officer, Chief Medical Officer, Chief Financial Officer, Chief Information Officer, and Chief Development Officer.

External Data Release (EDR) Tool is the Company-designated workflow tool used to submit and inventory a request to release Company Data to an External Entity and the subsequent approval or denial of the request by the appropriate Responsible Officer and/or the Value Management Committee.

External Entity is any third party not owned or operated by HCA Healthcare or its subsidiaries or affiliates (e.g., company, agency, vendor, consultant, educational institution, publication, Website/Internet).

Federal and State Reporting pertains to the submission of hospital data mandated by state/federal legislatures on a recurring schedule. State initiatives may include inpatient, ambulatory, emergency department, outpatient, and epidemiology information with many states mandating more than one type of submission. Federal Reporting would involve all data requests related to Federally-administered healthcare programs such as Medicare.

Health Care Operations means any of the following activities of the covered entity to the extent that the activities are related to covered functions (i.e., functions the performance of which makes the entity a health plan, health care provider, or health care clearinghouse):

1. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;
2. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;
3. Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable;
4. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
5. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary

development and administration, development or improvement of methods of payment or coverage policies; and

6. Business management and general administrative activities of the entity, including, but not limited to:
   (i) Management activities relating to implementation of and compliance with the requirements of this subchapter;
   (ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer;
   (iii) Resolution of internal grievances;
   (iv) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and
   (v) Consistent with the applicable requirements of § 164.514, creating de-identified health information or a limited data set and fundraising for the benefit of the covered entity.

Information Protection and Security (IPS) is the Department at the Corporate office responsible for information protection and security.

Intellectual Property (IP) is creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce. IP is protected in law by, for example, patents, copyright and trademarks, which enable people to earn recognition or financial benefit from what they invent or create. A Professional Services Agreement should be required when disclosing IP.

Lines of Business include, but not limited to, hospitals, ambulatory surgery centers, imaging and oncology centers, physician practices, shared services centers, corporate departments, Groups, Divisions and Markets (collectively with HCA Healthcare, the “Company”).

Payment is activities undertaken by a health care provider to obtain reimbursement for the provision of health care. Examples include, but are not limited to: determining eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts); billing, claims management, collection activities, obtaining payment; reviewing health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services.

Personally Identifiable Information (PII) is information that can be used alone or with other sources of information to uniquely identify, contact, or locate an individual.

Protected Health Information (PHI) is any oral, written or electronic individually-identifiable health information collected or stored by a facility. Individually-identifiable health information includes demographic information and any information that relates to past, present or future physical or mental condition of an individual. PHI excludes individually identifiable health information:

(i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
(ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv);
(iii) In employment records held by a covered entity in its role as employer; and
(iv) Regarding a person who has been deceased for more than 50 years.

Recurring Data Set is a Data Set that is contained in multiple files with fixed content, which may be provided to an External Entity on a recurring basis, whether defined by time period, patient class, geography or otherwise, but for which the delivery does not qualify as Streaming Data.

Registries are organized systems that use observational study methods to collect uniform data (clinical and other) to evaluate specified outcomes. (e.g., Cancer Registry, Death Registry, Medical Device Registries).

Release of Data is the disclosure, transfer, provision of access to, or divulging in any other manner of information outside of HCA-affiliated facilities or lines of business holding the information.

Request is a submission made within the External Data Release tool for sharing Company Data with external parties.

Research means a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge. [45CFR46.102(b)]. Research may also be a "clinical investigation" as defined by the FDA meaning "any experiment that involves a test article and one or more human subjects and that either is subject to requirements for prior submission to the Food and Drug Administration…or is not subject to requirements for prior submission to the Food and Drug Administration but the results of which are intended to be submitted later to, or held for inspection by, the Food and Drug Administration as part of an application for a research or marketing permit." [21CFR50.3(c)]

Responsible Attorney is the accountable Legal Counsel who ensures that the appropriate contractual provisions and documents are in place prior to releasing Company Data to external entities. Responsible Attorneys are trained on Data value and contractual protections.

Responsible Officer is any Chief Financial Officer (CFO) at a facility, division, or line of business, Corporate Senior Vice President (SVP), or Corporate Vice President (VP) who is authorized to approve certain Access and Approved Value Sharing Arrangements as described in this Policy. Other individuals may be designated by the VMC, from time to time, as the Responsible Officer for a specific Data Set. Responsible Officers are trained on Data value, management, and protection.

Restricted Use of Data is the External Entity's use of Company Data restricted such that the Data Set in question will be (a) *used by the External Entity for the expressly limited purpose of delivering the specific goods or services to the Company for which the Access to the Data Set was granted*, (b) owned at all times by the Company, (c) held separately by the External Entity without any intermingling, mixing or combining of such Data with other information, and (d) subject to the standard Company contractual terms with respect to retention, security, etc.

Senior Responsible Officer is an individual designated as a Responsible Officer that includes operational oversight for one or more Responsible Officers within that individual's line of business (e.g., a division CFO is the Senior Responsible Officer for facility CFOs; a group CFO is the Senior Responsible Officer for division CFOs).

Single Data Set is a Data Set contained in a single file, with fixed content. The Data Set is not updated, refreshed or expanded.

Sponsor is the individual submitting the request to release Company Data to an External Entity; usually a Company-affiliated management representative with direct knowledge of the business purpose/justification for the request.

Streaming Data is provided to the External Entity on a continuous or steady basis, but for which the delivery does not qualify as a Recurring Set.

Treatment is the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for healthcare from one health care provider to another.

Unrestricted Use of Data allows the External Entity to use Company Data in the development or delivery of services, products, or goods benefitting non-HCA Healthcare customers, clients, etc. This type of use is rare and requires approval from the Value Management Committee.

Value Management Committee (VMC) is the governing body responsible for oversight of this policy. It was created by the HCA Healthcare Executive Governance Committee (EGC). The VMC reviews Requests as specified in the Policy and approves or denies after evaluation of the risks and benefits to the business. The Committee is responsible for exploring the monetization of HCA Healthcare's data assets, evaluating requests to release data externally, and understanding opportunities to strengthen our data position to enable collaboration opportunities. The Committee has representation from across the Company. The voting members are: Chief Health Information Officer, Outpatient Services Group President, SVP Treasury & Finance, and SVP Chief Development Officer.