



A Taxonomy of Definitions for the Health Data Ecosystem

May 2019



**FUTURE OF
PRIVACY
FORUM**



THE Information
Accountability
Foundation
COLLABORATIVE POLICY INNOVATION

About FPF and IAF

Future of Privacy Forum is a nonprofit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. FPF brings together industry, academics, consumer advocates, and other thought leaders to explore the challenges posed by technological innovation and develop privacy protections, ethical norms, and workable business practices.

Information Accountability Foundation is the preeminent global information policy think tank that successfully works with regulatory authorities, policymakers, business leaders, civil society and other key stakeholders around the world to help frame and advance data protection law and practice through accountability-based information governance. Our goal, through active consultations and research, is to achieve effective information governance systems to facilitate information-driven innovation while protecting individuals' rights to privacy and autonomy.

Authors

Stanley Crosley – Senior Fellow, Future of Privacy Forum; Senior Foundation Strategist, Information Accountability Foundation

Carson Martinez – Policy Fellow, Future of Privacy Forum

Table of Contents

Introduction	1
Stakeholders	3
Data Categories	17
Data Uses and Purposes	29
Actions Performed on Data.....	34

Introduction

Healthcare technologies are rapidly evolving, producing new data sources, data types, and data uses, which precipitate more rapid and complex data sharing. Novel technologies—such as artificial intelligence tools and new internet of things (IoT) devices and services—and providing benefits to patients, doctors, and researchers. Data-driven products and services are deepening patients' and consumers' engagement, and helping to improve health outcomes. Understanding the evolving health data ecosystem presents new challenges for policymakers and industry ranging from health insurance companies already deeply entrenched in the health sphere to IoT companies just beginning to enter it. As the ecosystem grows, there is an increasing need to better understand and document the stakeholders, the emerging data types and their uses within this new and dynamic health data ecosystem.

In light of this need, the Future of Privacy Forum (FPF) and the Information Accountability Foundation (IAF) partnered to form the FPF-IAF Joint Health Initiative in January 2018. The goal of the Initiative was to create a framework to enable a better understanding of the current state of the health data ecosystem in one common language and to anticipate where it is heading. This report represents a culmination of collaboration, research, and discussions within a cross-functional group of leaders in industry, privacy, policy, and others, to fulfill this goal.

To analyze and create a cohesive taxonomy of the collection and use of health data across the wide variety of stakeholders, the project team was informed by FPF's and IAF's work in health privacy, de-identification, artificial intelligence, and IoT. We also benefitted from Initiative members' expertise and experience within the ecosystem. The *Taxonomy of Definitions for the Health Data Ecosystem* is intended to enable a more nuanced, accurate, and common understanding of the current state of the health data ecosystem. The Taxonomy outlines the established and emerging language of the health data ecosystem. The Taxonomy lists and defines:

- (1) **Stakeholders:** The Taxonomy describes stakeholder types currently involved in the health data ecosystem and identifies examples;
- (2) **Data Categories:** The Taxonomy identifies common and emerging data types that are being collected, used, and shared across the health data ecosystem;
- (3) **Data Uses and Purposes:** The Taxonomy provides baseline definitions regarding the purposes for which data types are used in the health data ecosystem; and
- (4) **Actions Performed on Data:** The Taxonomy classifies the types of actions that are now being performed and which we anticipate will be performed on datasets as the ecosystem evolves and expands.

Although the document is largely US-focused, global terms and definitions were considered and included in the taxonomy where possible—we anticipate that terms may be used across borders. Additionally, relevant regulations and laws, including the General Data Protection Regulation (GDPR),¹ the California Consumer Privacy Act (CCPA),² the Health Insurance Portability and Accountability Act (HIPAA),³ the Common Rule,⁴ and the Genetic Information Nondiscrimination Act (GINA)⁵ are noted throughout the document when they share overlapping terminology and definitions.

This report is an educational resource that will not only enable a deeper understanding of the current landscape of stakeholders and data types. We hope it will be valuable as a common, reference language for the evolving health ecosystem. This is particularly important as organizations begin to take on more data governance projects, take inventory of the data flowing into and out of their organizations, and participate in complex data exchanges. We intend the Taxonomy to be used to create consistent data collection and use models across the healthcare ecosystem. Establishing common, shared terminology is particularly useful as state privacy laws and pending Congressional proposals seek to codify a comprehensive consumer privacy framework in the United States and include enhanced transparency provisions that would require companies to undertake data mapping and inventory activities.

Most of these emerging proposals include requirements that companies provide consumers with details about: the categories of personal information collected, shared, and disclosed; the purposes for which personal information is used; and the third parties with whom they share data. This Taxonomy provides a practical foundation for companies to standardize within their organization and across departments the language used for mapping data flows and taking inventories of data sources, data types, and processing activities.

For additional information about this Taxonomy or the Joint Health Initiative work between the Future of Privacy Forum and Information Accountability Foundation, please contact Stan Crosley (stan@crosleylawoffices.com) and John Verdi (jverdi@fpf.org).

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [hereinafter GDPR].

² California Consumer Privacy Act of 2018 (CCPA), Cal. Civ. Code § 1798 (2018) [hereinafter CCPA].

³ Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, 110 Stat. 1936 (1996); 45 C.F.R. § 160, § 164 (2002) [hereinafter HIPAA].

⁴ Protection of Human Subjects, 45 C.F.R. § 46 (2005) [hereinafter Common Rule].

⁵ Genetic Information Nondiscrimination Act of 2008, Pub. L. 110-223, 122 Stat. 881, Title II codified at 42 U.S.C. 2000ff et seq. (2008) [hereinafter GINA].

Stakeholders

Academic or University Researcher: An individual who or organization that participates in systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge⁶

Accreditation Organization: An authoritative body that determines through an assessment process whether a third party meets or conforms to standards (the accreditation) and demonstrates competence to maintain those standards⁷

Examples: Joint Commission on Accreditation of Healthcare Organizations (JCAHO), National Committee for Quality Assurance (NCQA), American Medical Accreditation Program (AMAP), Utilization Review Accreditation Commission (URAC)

Adverse Event Reporting Organization: An organization that collects information on a mandatory or voluntary basis regarding pathological bodily process that is induced by or linked to a medical intervention

Examples: MedWatch/FDA Adverse Event Reporting System, (FAERS), HHS Vaccine Adverse Event Reporting System (VAERS), Massachusetts Serious Reportable Events (SRE), European Database of Suspected Adverse Drug Reaction Reports

Advertising Exchange: A company that hosts an online marketplace/platform that facilitates the buying and selling of media advertising inventory or ad impressions between exchange participants, including advertisers, publishers, and networks⁸

Examples: DoubleClick, AOL's marketplace, AppNexus, OpenX

Advertising Network: A company that sells inventory across a range of publisher websites to advertisers wishing to buy ads on those websites

Examples: Google AdSense, Media.Net, BuySellAds, Conversant

⁶ 45 C.F.R. § 46.102

⁷ ISO/IEC 17011: "Conformity assessment. General requirements for accreditation bodies accrediting conformity assessment bodies" (2004). <https://www.iso.org/obp/ui/es/#iso:std:iso-iec:17011:ed-1:v2:en>

⁸ "IAB Glossary: Digital Media Buying & Planning." <https://www.iab.com/wp-content/uploads/2016/04/Glossary-Formatted.pdf>

Affiliate Company: A company that is directly or indirectly being controlled by or under common control with another entity or company; the other entity or company must own less than a majority of the voting stock of the other

Authorized Decision-Maker: (*Also known as a Surrogate or Patient Representative*) An individual who assumes decisional authority for a patient who lacks decisional capacity; this individual can be appointed through the judicial system or prospectively authorized by the patient at a time when he or she had decisional capacity. HIPAA uses the term “patient representative” and defers to state law for the appropriate determination of who can be a patient representative⁹

Biobank: Any organization that collects human biological samples and linked data that is to be used for research purposes¹⁰

Examples: Autism Genetic Resource Exchange, Mayo Clinic Biobank, Duke Biospecimen Repository & Processing Core, Manhattan HIV Brain Bank

Call Center (Medical): A communications center that manages incoming and outgoing telephone calls with customers and clients to aid in billing, collections, appointment making, and providing healthcare information

Examples: Ashfield Healthcare Communications, Sequence Health

Caregiver: An individual who is involved in arranging and helping with the care of a patient. Sometimes can also be the Patient Representative

Examples: Spouse, Child, Relative, Friend of a Patient

Contract Research Organization (CRO): An organization hired by a pharmaceutical, biotechnology, medical device company, or research center to take over certain parts of running a clinical trial by designing, managing, or monitoring the trial, and analyzing the results¹¹

⁹ DeMartino, S.E. et al (2017) “Who Decides When a Patient Can’t? Statutes on Alternate Decision Makers.” N Engl J med. 376(15): 1478-1482.

¹⁰ Shaw, D.M.. (2014). “What is a biobank? Differing definitions among biobank stakeholders,” *Clinical genetics*, 85(3), 223-227.

<https://pdfs.semanticscholar.org/6214/09329391228dbfdc8937a5a75e3fe09350ad.pdf>

¹¹ National Cancer Institute (NCI) Dictionary of Cancer Terms.

<https://www.cancer.gov/publications/dictionaries/cancer-terms/def/contract-research-organization>

Examples: IQVIA, Syneos Health, Paraxel International Corporation, PRA Health Sciences, Covance

Cloud Service Provider: A company that owns and operates cloud-based infrastructure, application, platform, or storage services, which can be made available publicly or privately to other businesses or individuals typically on a pay-per-use model

Examples: Microsoft Azure, Amazon Web Services (AWS), Google Cloud Platform, IBM Cloud, Oracle, Salesforce

Compounding Pharmacy: A pharmacy that combines, mixes, or alters ingredients of a drug to create a medication prescribed by a provider and tailored to the needs of an individual patient, which cannot be met by commercially available products. Compounding Pharmacies are required to have specialized license approvals

Consumer: Individual who interacts with a company/entity through public-facing media or devices, such as websites, mobile apps, call centers, but who in such interactions is not a patient currently using such products or services. E.g., a user of a biopharmaceutical company website

Example: Website Visitor

Consumer Genetic Testing Company: A company that offers consumer genetic or personal genomic testing services to a consumer without the involvement of a healthcare provider or health insurance company

Examples: 23andMe, Helix, Ancestry, Habit, MyHeritage, African Ancestry, Living DNA, FamilyTreeDNA

Consumer Laboratory Services Company: A company that offers laboratory testing services of human specimens to a consumer without the involvement of a healthcare provider or health insurance company (also known as "Direct Access Testing")¹²

Examples: Quest Diagnostics, Laboratory Corp, Counsyl, MyMedLab

Data Donor: An individual who shares their data and history with another (organization or individual) for research or other defined purposes. HIPAA permits an

¹² Centers for Medicaid and Medicare (CMS). "Direct Access Testing (DAT) and the Clinical Laboratory Improvement Amendments (CLIA) Regulations." <https://www.cms.gov/regulations-and-guidance/legislation/clia/downloads/directaccesstesting.pdf>

individual to direct a Covered Entity to send the individual's PHI to a third party, which is being used as a way to facilitate data donation

Examples: Consumer, Patient, Clinical Trial Participant

Data Aggregation/Analytics Service: An organization that provides data analytics software and operations to or performs data analytics services for another entity

Examples: Optum, Cerner, Acxiom, HealthEC, Philips Wellcentive, Arcardia, SICO Health Analytics, CoreLogic, Datalogix, eBureau, ID Analytics, Intelius, PeekYou, Rappleaf, Recorded Future, IQVIA, PatientsLikeMe

Data Informatics Scientist: (Also known as Data Informaticist) An individual who specializes in the design, development, adoption, and application of IT-based innovations with respect to data and information

Data Management Platform Vendor: A company that provides software and a centralized system for collecting, organizing, and analyzing large sets of data originating from disparate sources

Examples: Oracle, Adobe, KBM, Rocket Fuel, Salesforce

Data Protection Authority (DPA): Dependent public authorities and/or governmental agencies that supervise, through investigative and corrective powers, the application of the data protection law in countries that have enacted comprehensive data protection legislation. In the EU, they provide expert advice on data protection issues and handle complaints lodged against violations of the General Data Protection Regulation and the relevant national laws¹³

Data Protection Officer: An officer designated by an organization who is responsible for ensuring compliance with data protection laws

Debt Collection Agency: A company that works to recover money owned on behalf of another individual or business, and typically collect debts for a fee or percentage of the total amount owed

Examples: Rocket Receivables, Summit AR, Aspen National Collections

¹³ European Commission. "What are Data Protection Authorities (DPAs)?" https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en

De-identification Company: A company that provides data de-identification and anonymization services and/or solutions

Examples: Anonos, Privacy Analytics, Universal Patient Key (UPK)

Digital Health Sensor Company: A company that researches, designs, manufactures, commercializes, and supports sensors or other data capture mechanisms for medical devices (or other collection medium) that utilize cloud-based or mobile software tools that collect and process health information from the user

Examples: Proteus, Butterfly iQ, AliveCor's Kardia EKG, Adherium AstraZeneca's Symbicort Smart Inhaler

Electronic Clinical Report Form (eCRF) Vendor: A company that offers auditable electronic record of information that generally is reported to the sponsor on each trial subject, according to a clinical investigation protocol. The eCRF enables clinical investigation data to be systematically captured, reviewed, managed, stored, analyzed, and reported¹⁴

Examples: Oracle/PhaseForward, Medidata, IBM, Innovate Research

Electronic Health Records (EHR) Company: A company that provides software applications that allows users to capture, access, organize, store, and share the electronic version of a patient's medical history in a structured format

Examples: Epic, Allscripts, eClinicalWorks, Athenahealth, NextGen Healthcare, McKesson, Cerner

Emergency/ Outpatient Care Center: An organization that serves as an alternative place to receive healthcare when an individual is unable to get to a hospital¹⁵

Emergency Contact: The individual a patient designates to be called in the case of an emergency

Expert Statistician: A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable¹⁶

¹⁴ Food and Drug Administration. (2013) "Guidance for Industry: Electronic Source Data in Clinical Investigations." <https://www.fda.gov/downloads/drugs/guidances/ucm328691.pdf>

¹⁵ Centers for Disease Control and Prevention (CDC) (2017) "Planning Resources by Setting: Outpatient Clinics and Urgent Care." <https://www.cdc.gov/phpr/readiness/healthcare/outpatient.htm>

¹⁶ 45 C.F.R. §164.514(b)(1)

Federal Trade Commission (FTC): The US federal agency that promotes consumer protection and the elimination and prevention of anticompetitive business practices. From a data protection perspective, the FTC relies on Section 5 of the FTC Act and the legal standards of deception and unfairness¹⁷

Formulary and Drugs Committee: A committee within a health care organization charged with reviewing and recommending which drugs require authorization, establishing policies regarding the use of drugs, therapies, and drug-related products, and identifying those that are most medically appropriate and cost effective to serve the organization's patient population¹⁸

Government Payer: A type of health plan in which the government provides or pays the cost of medical care

Examples: Medicaid, Medicare, CHIP

Government Health Authority/Agency: A government agency or authority that is responsible for health matters as part of its official mandate

Examples: Department of Health and Human Services (CDC, CMS, FDA, HRSA, AHRQ, NIH, SAMHSA, ONC, Veterans Health Administration), Federal Bureau of Prisons (Health Services Division), European Medicines Agency, European Research Council, European Centre for Disease Prevention and Control

Healthcare Clearinghouse: A public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches that either process or facilitate the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction, or receive a standard transaction from another entity and process or facilitate the processing of health information into a nonstandard format or nonstandard data content for the receiving entity

Examples: Apex EDI, Navicure, Claim MD, PracticeSuite, Availity

Health Information Exchange: The implementation of technologies/services that allow health care professionals and services companies to exchange health data in

¹⁷ 15 U.S.C. § 45(a)

¹⁸ American Society of Health-System Pharmacists (ASHP) (2008) "ASHP Guidelines on the Pharmacy and Therapeutics Committee and the Formulary System." <https://www.ashp.org/-/media/assets/policy-guidelines/docs/guidelines/gdl-pharmacy-therapeutics-committee-formulary-system.ashx?la=en&hash=EF1E4214CC91C65097AEECE91BF6EC985AE3E56>

standardized formats to facilitate messaging and other functionality and to more easily permit health care providers to appropriately access and securely share a patient's medical information electronically with the patient and others

Examples: Allscripts dbMotion Solution, Cerner Network, Change Healthcare Clinical Exchange HIE, eClinicalWorks, Medcity HIE, Indiana Health Information Exchange

Health Insurance Company: (Also known as a Private Payer) Individual and group plans that provide or pay the cost of medical care, which can include a health, dental, vision, and prescription drug insurers; health maintenance organizations; disability insurer; employer-sponsored health insurer; life insurer; and long-term care Insurer

Examples: Highmark, Unitedhealth, Aetna, Kaiser Foundation, Wellpoint, Anthem, Blue Cross/Blue Shield, Cigna, Humana, Carefirst, Coverntry

Healthcare Provider (HCP): A person, company, or other entity that provides medical or health care services to an individual

Examples: Doctors, Clinics, Psychologists, Dentists, Chiropractors, Nursing Homes, Pharmacies.

Hospice: An organization that provides a type of palliative care that may be offered during the terminal stage of illness when no further therapy is available or when the patient or authorized decision maker no longer wants to pursue therapy

Hospital/Clinic: An institution with an organized medical or other professional staff that provides medical, surgical, and other treatment to a patient

Examples: Cleveland Clinic, Mayo Clinic, Johns Hopkins Hospital, Ronald Reagan UCLA Medical Center

IT Infrastructure Company/Vendors: A company that provides a portion or all of the technology that underpins an organization's software, processes, and operations

Examples: Optum, Cerner, GE, Epic, Mckesson, Leidos, IBM, Microsoft, Intel, Seimens, Royal Philips, Nebula Genomics, Medicalchain, Iryo, Doc.AI

Installed Medical Device/Device Servicing Entity: A medical device company that provides devices, equipment, products to health care providers for installation and use in the HCP offices (including hospitals) and typically referring to "smart" or connected

devices, such as imaging machines, respirators, smart beds, etc. Compare to “patient medical device” entities that provide medical devices worn, embedded in, or attached to the patient

Examples: Abbott, GE Health, Hill-Rom, J&J, Philips, Siemens, and thousands of others and growing as traditionally manufactured products embed sensors and become connected (e.g., hospital beds)

Institutional Review Board (IRBs): *(Also known as Ethical Review Board or an Ethics Committee)* A group of people who review, approve, and monitor a research study's protocol. Their role is to protect the rights and welfare of people participating in a study. The group typically includes people with varying backgrounds, including a community member, to make sure that research activities conducted by an organization are completely and adequately reviewed. Reviews by IRB/ERB/ECs are required in most countries where a study sponsor desires to obtain marketing approval for a health product or where the research is to be used to add to generalized knowledge (see the Common Rule)¹⁹

Examples: Academic IRBs, private IRBs (e.g. Quorum Review, Western, Schulman, New England Independent Review, CIRCARE)

Journal/Publication Entity: A periodical publication intended to further the progress of a discipline by reporting new; can be scholarly or peer-reviewed

Examples: Science, Nature, New England Journal of Medicine, European Journal of Public Health, JAMA, Cell, PLOS One, Proceedings of the National Academies of Sciences

Lab Services Company: A company that offers laboratory testing services of human specimens in order to obtain information about the health of a patient with a healthcare provider or health insurance company in the process

Examples: LabCorp, Myriad Genetics, Quest Diagnostics, Siemens Healthineers, Alere, DaVita Healthcare Partners

Market Research Agency: A company that gathers, analyzes, and interprets information about a market, product or service within the market, and customers of the product or service

¹⁹ US National Library of Medicine. Glossary of Common Site Terms. <https://clinicaltrials.gov/ct2/about-studies/glossary>

Examples: IQVIA, Kantar, Nielsen, IRI, Westat

Marketing Company: A company involved in creation, communication, delivery, and/or exchange of offers that have value for customers, clients, and partners, including direct to consumer pharmaceutical advertisers and healthcare provider advertisers

Examples: PWC Digital Services, Epsilon, IBM iX, Acxiom, IPG, Deloitte Digital, Accenture Interactive, Pfizer, Merck, AbbVie, Allergan, AstraZeneca, Novartis

Managed Care Organization: A company that produces an object or component that is used in the diagnosis, treatment, prevention, or cure of medical conditions or diseases or affects body structure of function through means other than chemical or metabolic reaction in humans²⁰

Examples: Novartis, 3M, Abbott Laboratories, Johnson & Johnson, Siemens, GE, Philips, Medtronic

Medical Device Processing Entity: Entities that research, design, manufacture, commercialize, and support processing chips and technology that enable data processing on medical and other health devices

Examples: Intel, Qualcomm, Nvidia, IBM, Samsung, Hewlett-Packard

Medical School/ University: An education institution that provides students a training a competency in the art and science of medicine that permits them to obtain a license to practice medicine and awards professional degrees to physicians and surgeons, such as Doctor of Medicine (MD), Bachelor of Medicine (MB), Bachelor of Surgery (SB), etc.

Examples: Harvard Medical School, Northwestern Feinberg School of Medicine

Mobile Application Provider/ Developer: An individual or company that is involved in the process of creating software for mobile devices

²⁰ Health, Center for Devices and Radiological. "Classify Your Medical Device - Is The Product A Medical Device?"
<https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/ucm051512.htm>

Examples: Appster, LeewayHertz, Zco Corporation, Eight Bit Studios, Y Media Labs

Mobile Communications Service Provider: A company that researches, designs, manufactures, commercializes, and supports mobile devices, such as smartphones, tablet computers, laptops, etc. that can connect to the internet and interconnect with other devices

Examples: Apple, Samsung, Google, LG, Lenovo, Nokia

Mobile Health (mHealth) Company: A company that researches, designs, manufactures, commercializes, and supports devices, applications, sensors, and other technologies that utilize cloud-based or mobile software tools to collect, use, analyze, transfer or otherwise process health information from the user of the mobile health device

Examples: Apple, AlivCor, Nike, Fitbit, Vodafone, Qualcomm, AT&T, Cerner, Honeywell, Athenahealth

Nonprofit Research Organization: A public organization that is primarily engaged in basic and/or applied research, the purpose of which is directed toward public benefit

Examples: PEW Charitable Trusts, Robert Wood Johnson Foundation, Broad Institute

Nursing Home/Facilities: A public or private organization that provides skilled nursing services, 24-hour supervision, rehabilitation, and long-term care

Patient: An individual who receives treatment or utilizes health care products or services, including medical devices, pharmaceutical products, or other therapies

Patient Advocacy Organization: An organization that advocates on behalf of patients, survivors, and caregivers often concerned with one specific group of disorders or conditions

Examples: American Diabetes Association, Lupus Foundation of America, National Osteoporosis Foundation, National Health Council

Patient Support Program (PSP): *(Also known as Patient Assistance Programs)* A service for direct patient or patient care interaction/engagement to help understand and/or facilitate reimbursement from payers, management of medication, and/or

disease outcomes (e.g. adherence, awareness, and education) or to provide healthcare providers with support for their patients²¹

Patient Network: A network/application/forum that provides patients and their families the ability to connect with others, track their progress and express their health status, often built around a particular condition or disease

Examples: Patientslikeme, IMedix, Inspire, Diabetic Connect

Payer: The entity other than the patient that finances or reimburses the cost of health services

Examples: Private Payer/Health Insurer, Government Payer, Employer Payer

Payment Adjudication Vendor: A company that is involved in or provides software for the process of paying or denying submitted claims after comparing them to the benefit or coverage requirements and notifying the claim submitter of the outcome

Examples: Co-pay Card Vendors, AssistRX

Personal Health Record (PHR) Provider: A company that provides an electronic application through which individuals can access, manage, and share their health information and that of others for whom they are authorized in a private and secure environment²²

Examples: Microsoft HealthVault, WedMD PHR

Pharmaceutical Company: A company licensed to research, discover, develop, produce, market, and/or distribute pharmaceutical drugs

Examples: Pfizer, Novartis, Jazz Pharmaceutical, Biogen Idec, Merck, Eli Lilly and Company, GlaxoSmithKline

Physical and Security Services: A company that provides physical, technical, and/or administrative safeguards (infrastructure, software, or otherwise) for another entity

²¹ ABPI Pharmacovigilance Expert Network (2011) "Guidance Notes for Patient Safety and Pharmacovigilance in Patient Support Programmes." <http://www.abpi.org.uk/media/1592/110504-final-abpi-pen-ppsp-guidance.pdf>

²² Connecting for Health. (2003) "The personal health working group final report." Markle Foundation. <http://research.policyarchive.org/15473.pdf>

Examples: ClearData, ID Experts, Protenus, Hashed Health, Medcrypt, Senrio, Cylera, Health Linkages

Physician/Provider Network: A panel of physicians, other healthcare providers, and hospitals that a third-party payer has contracted with to provide medical care to enrollees in the payer's health plan

Professional and Membership Associations: A nonprofit organization that seeks to further a particular profession, the interests of individuals engaged in that profession, and public interest

Examples: American Society of Anesthesiologists, Academy Health, Research!America, Medical Device Manufacturers Associations (MDMA)

Primary Care Doctor: A physician who provides definitive care to a patient at the point of first contact, and takes continuing responsibility for providing the patient's comprehensive care

Examples: Family Medical Doctor, Internal Medicines Doctor, Pediatrician

Public/Open Data Platform: An organization that provides and promotes open data for collaborative data analysis

Examples: Sage bionetworks, Big Cities Health Inventory Data Platform

Research Participant/Human Subject: A living individual about whom an investigator conducting research obtains (1) data through intervention or interaction with the individual, or (2) identifiable private information about whom includes a subject's opinion on a given topic²³

Examples: Consumer, Patient

Retail Pharmacy: A pharmacy that is licensed to sell and dispense medications to the general public at retail prices

Examples: CVS, Walgreens, Walmart, Rite Aid, Kroger, Target

²³ 45 C.F.R. § 46.102

Social Media Company: A company that provides platforms/applications/and other services to the general public to facilitate social interaction between individual

Examples: Twitter, Facebook, Instagram, Snapchat, Youtube, Pinterest, Reddit, LinkedIn, Tumblr, Flickr

Specialty Pharmacy: A pharmacy focuses on high cost, high complexity medications and therapies for patients with complex disease states

Examples: CVS Pharmacy Specialty Services, Alliance Rx Walgreens Prime, BrivoRx, Humana Specialty Pharmacy, Cigna Specialty Pharmacy

Specialty Care Doctor: A physician who holds advanced training and has been board certified in a particular branch of medicine, and provides care to a patient who has been referred from a primary care doctor

Examples: Neurologists, Radiologist, Psychiatrists, Oncologists, Dermatologists, Orthopedic Surgeon, Endocrinologist

Specific Reimbursement Authorities: Reimbursed products v hospital products (public procurement—different bodies); sometimes a part of the hospital, sometimes a different authority

Telehealth/Telemedicine Company: A company that creates electronic information and telecommunication technologies that allow long distance patient/clinician contact and care, advice, reminders, education, intervention, monitoring, and remote admissions

Examples: CareClix, ConsultADoctor, Teladoc, MeMD, iCliniq, American Well, MDLIVE

Technology Company (non-medical): A company that develops and/or manufactures technology or provides technology as a service to another entity.

Examples: Apple, Google, Toyota, Amazon, GM, Garmin (each of these entities can also be a digital or mobile health company)

Vendor/Service Providers: A company or entity that acts under the direct authority of the data controller or processor and are authorized to process personal data in support of providing the data controller's commercial product or service²⁴

Workforce: A group of persons that conducts services and actions for a company and is under the direct control of that company²⁵

²⁴ The CCPA defines a service provider as: "A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business." See: Cal. Civ. Code § 1798.140(v)

²⁵ HIPAA defines workforce as: "employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate." See: 45 C.F.R. § 160.103.

Data Categories

Adverse Event Data: Data associated with an untoward medical occurrence in a patient, such as any unfavorable and unintended sign (e.g. an abnormal laboratory finding), symptom, or disease temporally associated with the use of a drug or medical product

Examples: Reaction Information from Reports, Patient Outcome Data, Drug or Medical Product Type and Information, Number of Cases

Advertising Identifier (Mobile Apps): A resettable, random identifier that mobile operating systems such as iOS and Android assign each device

Biometric Data: Unique and identifying Information resulting from the specific technical processing relating to the physical, physiological, or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person²⁶

Examples: Full Face, Fingerprint, Retinal Scan, Heartbeat

Biospecimen Data: Data related to the physical sample of tissue, blood, urine or other biologically derived material taken from a patient and its processing

Examples: Biological Sample IDs or Codes, Specimen Characterization Data, Linked Identifier Information

Blood Type: Data related to the type of blood a patient holds

Examples: A (+/-), B (+/-), AB, or O

Browsing History Data: List of websites viewed through server/device

²⁶ The GDPR defines biometric data as: "Personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data." See: GDPR, Art. 4(15); The CCPA defines biometric data as: "An individual's physiological, biological or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information." See: Cal. Civ. Code § 1798.140(b).

Examples: Browsing/View History Specific to Browser, or Captured by Browser's Capabilities

Business Contact Data: Data that can be used, by itself, to contact a business

Examples: Business Name, Physical Address, Phone Number (landline, cellphone), Email Address

Call Detail Records: (Also known as Cellphone Metadata) A record produced by the electronic communications between cellphones (calls or messages)

Examples: Originating and Recipient Phone Numbers, Originating and Recipient Cell Tower Locations, Call or Message Starting Time and Duration, Telephone Serial Numbers

Claims Data: Data related to the financial interactions between insured patients and the healthcare delivery system

Examples: Inpatient, Outpatient, Enrollment, Patient Claims from Government or Commercial Health Firms

Clinical Decision Support (CDS) Data: Data derived from systems that assist healthcare providers in making medical decisions. These systems require inputs from patient-specific variables, and after comparisons and analysis, output specific patient recommendations

Clinical Trial Data: Data generated from a human subject research study involving one or more human subjects that are assigned to an intervention(s) to evaluate the effects, tolerability, safety, and efficacy of that intervention(s) on health-related biomedical or behavioral outcomes

Examples: Individual Participant Data; Summary Level Results and Trial Findings; Patient Reported Outcomes; Safety and Efficacy of a Drug, Device, or Biologic; Dose-Ranging; Interaction and Adverse Events; Trial Phase Related Information

Cloud Service Provider Data: System maintenance data, which includes no customer information

Examples: Cloud service provider passwords, authentications, service logs

Company-Generated ID: Company-generated identifier associated with data about a specific individual

Examples: Ad Identifier, account number, customer number

Contact Data: Data that can be used, by itself, to contact an individual

Examples: Name, Physical Address, Email Address, Phone Number (landline, cellphone)

Cookie: A small text file that a website places on a user's browser, which are then sent back in internet traffic to enable personalized online experiences and can enable websites track browser activity, remember user preferences, keep users logged in for subsequent sessions, etc.

Contact Data – App Messaging: Data that can be used, by itself, to contact an individual through application-based messaging

Examples: User-handles on Facebook, Twitter, Instagram, Pinterest, Snapchat, Tinder, Houseparty, GroupMe, Kik, Vibr, LinkedIn, Skype, iMessage, YouTube, Google+, etc.

Contact Data – Email: Data that can be used, by itself, to contact an individual by email

Example: Email address

Contact Data – Mobile: Data that can be used, by itself, to contact an individual on mobile devices

Example: Phone Number

Contact Preferences: Data entailing the mode, but not content, of past interaction, as well as individual provided preference for mode of future interaction

Examples: Preferences for Email, Text Messaging, Phone, Applications

Content Consumption Data: List of media content viewed through server/device

Examples: Television, E-Book, Music, Movie Downloads

Credential Data: Data provided by an individual, to identify that individual to a device, app, website, or service

Examples: UserID, Password, Challenge Question, Fingerprint, (SSN, DLN)

Customer Contact List Data: Customer provided contact information for others

Examples: Contact list [e.g. "address book"], Family Grouping from Third-Party but Imported into Device

Demographic and Socioeconomic Data: Data entailing personal social details which do not, on their own, reveal the identity of individual, gathered through the capabilities of the app or cloud surface

Examples: Age, Gender, Marital Status, Number of Children, Household Income, Census Records, Birth Country, Citizenship, Race/Ethnicity, Birthdate

Diagnosis Data: Data related to the determination of a condition or disease that has caused a patient's symptoms and sign

Disaster Recovery Data: Broad data collected as a way to prevent large-scale and total data loss

Examples: Offsite Server Backups, Transaction Logs

Drug or Product Label Data: Data related to information included in drug or product labels prepared by manufacturers and approved by the FDA

Examples: Prescriber name, pharmacy name and address, patient name and address, prescription number, dosing and administration, number of refills, expiration data, instructions and usage, warning and precautions, adverse reactions, and drug interaction

Education Data: In health ecosystem, generally data related to the academic degrees obtained, honors or awards from an academic institution, and the academic institutions attended by health care professionals, or at which the HCP teaches

Examples: Information about Academic Degrees, Honors, Awards, Attendance (Including Dates of Attendance), Graduation, Teaching Assignments

Electronic Health Record/Electronic Medical Record data (EHR/EMR): Health Data maintained in an electronic record repository controlled by a health care provider. In some contexts, an EHR is seen as being a broader record category with data more expansive than an EMR

Examples: Full or Segments of Health Records of a Health Care Provider

Environmental Data: Data derived from the observation or measurement of the elements, features, and state of the environment in which an individual resides, works or frequents. Data can be in written, visual, audio, electronic, or any other form. It is

commonly used as a means to express the need to gather data about the way an individual lives

Examples: Air Quality, Population Characteristics, Climate, Poisonings, Toxic Releases, Radiation Exposure Levels, Atmospheric Pressures, Biological Diversity

Epidemiological Data: Data arising from the study of the distribution and determinants of health-related states or events (including disease). Epidemiological data is used to study the control of diseases and other health problems. Epidemiological Research is also sometimes called Records-based research since it involves the study of data that is already part of the Electronic Health Record or similar set of data²⁷

Family Health History Data: Health Data surrounding the health of an individual's family

Examples: Health Concerns Present in Family Members, Risk of Disease Factoring in family History, List of Diseases, Illnesses, Allergies, Surgical Procedures

Financial Data: Data provided by user to pay for services or make purchases within the server/app

Examples: Payment Instrument Data, Credit Card Data, Financial Status, Loans, Bank Account Information

Fraud Data from 3rd Party: Specific data collected by 3rd party entities to patrol attempted user fraud

Examples: Return Offenders, Fraudulent Claims, Stolen Credentials

Genetic Data: Personal data that concerns information about an individual's inherited or acquired genetic characteristics²⁸

²⁷ Tyler C.W., Jr and J.M. Last, "Epidemiology" (1991), in J.M. Last, R.B. Wallace, eds., *Maxcy-Rosenau-Last Public Health and Preventive Medicine*, 13th ed.

²⁸ The GDPR defines genetic data as: "Personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained." See: GDPR, Art. 4(13); GINA defines genetic data as: "With respect to any individual, information about--
(i) such individual's genetic tests,
(ii) the genetic tests of family members of such individual, and
(iii) the manifestation of a disease or disorder in family members of such individual."

See: 42 U.S.C. § 2000ff-4(a)

Examples: Genome Sequences, Single Nucleotide Polymorphisms (SNPs), Genome Wide Association Study (GWAS) Data, Genetic Disease Diagnosis/Risk Analysis, Genetic Biomarkers, Genotypic Data, Phenotypic Data

Geolocation Data: Data utilizing GPS technology of device or cloud-service for gross location services, directions, or app-specific recommendations/add-ons that indicates the geographical position

Examples: Latitude/Longitude, Zip code, State, City, [e.g. Precise, Near, etc.]

Health Care Utilization Data: Data about a population's use of available healthcare services and resources

Health Data/Information: Data relating to the physical or mental health an individual, or the provision of services relating to the physical or mental health of an individual, entailing general health observations and potential records of diagnoses, procedures, and treatments²⁹

Examples: Weight Fluctuations, Pain Levels, HB1C Measurements, Heartrate Measurements

Health Insurance Information: Data relating to a patient's health insurance plan, including long-term care, disability, or other health plans³⁰

Examples: Insurer, Type of Coverage, Claims, Deductible, Premium, Co-pay, In Network and/or Out of Network Providers, Out-of-Pocket Max, Coinsurance, Member ID

²⁹ GDPR defines "data concerning health" as: "Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status." See: GDPR, Art. 4(15); HIPAA defines "Individually identifiable health information" as: "Information that is a subset of health information, including demographic information collected from an individual, and:

- (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
- (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
 - (i) that identifies the individual; or
 - (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual."

See: 45 C.F.R. § 160.103.

³⁰ The CCPA defines health insurance information as: "A consumer's insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the consumer, or any information in the consumer's application and claims history, including any appeals records, if the information is linked or reasonably linkable to a consumer or household, including via a device, by a business or service provider." See: Cal. Civ. Code § 1798.140(k).

Health System Capacity Data: Data relating to the distribution of healthcare resources, including hospital capacity and labor capacity

Examples: Number of General and Intensive Care Beds, Imaging Devices, Procedure Suites, Physicians, Nurses, Administrative Staff and Other Health Professionals Available

Interests Data Categories: Data provided or acquired about individual's interests and preferences revealing lifestyle patterns and habits, which do not, on their own, reveal the identity of individual

Examples: Golf, Cooking, Reading, Travel, Healthy Living

IP Address: The Internet Protocol Address, which is an Identifier assigned to every internet-connected device on a network at a given point in time, to enable that device to send and receive internet traffic

Laboratory Results: Data derived from the analysis of biospecimens intended to detect, identify, or quantify a substance(s), evaluate function or response to treatment, establish the nature of a condition or disease, or plan treatment, among others

Examples: Order Number; Patient Name and Identification Number; Test Report Date; Provider; Name of Test; Biospecimen Data; Report Outcomes, Which Can Include Reference Ranges, Positive or Negative, Substance Identification, Unit of Measurement; Abnormal Results

Legal Requests: Data chronicling current, past and possibly future legal actions

Examples: Law Enforcement Investigations, Discovery Requests

Marketing/Ad Campaign Data & History: Individual provided subjective responses, and marketing interactions collected by web-servers

Examples: DM Campaigns, Ad Impressions, Response to Marketing/Ads

Medical Device Data: Data that has been recorded, stored, processed, retrieved, and/or derived from a medical device³¹

³¹ Food and Drug Administration, "Manufacturers Sharing Patient-Specific Information from Medical Devices with Patients Upon Request – Guidance for Industry and Food and Drug Administration Staff", available at <https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM505756.pdf>

Examples: Device Usage/Output statistics, Healthcare Provider Inputs, Records of Malfunctions or Failures, Incidence of Alarms

Medical History Data: Information about a patient's past and present health gathered by a physician through Q&A

Examples: Allergies; Illness, Surgery, and Procedure History; Social History; Family Health; Medications Taken; Sexual History; Present Diagnosis or Complaints; Weight; Height; Emergency Contact Information

Medical Imaging Data: Unstructured data derived from technologies used to view the human body in order to diagnose, monitor, or treat medical conditions

Examples: Radiographic Images, MRIs, Ultrasound or Sonographic Images, Computed Tomography, PET, and X-Ray Images, and Associated Metadata

Medical Information Request: Any unsolicited written, electronic, or oral request for medical and/or scientific information regarding Company products from any source, including from HCPs, patients, or consumers

Mortality Data: Data concerning the death of a patient or group of patients

Examples: Name, Sex, Age, Familial Information, Date and Time of Death, Cause of Death, Demographic Information, Geographic Information, Autopsy Information

Movement Data: Data utilizing GPS technology of device or cloud-service, to track minute changes in location and activity levels (e.g. step tracker or user-entered exercise data)

Examples: Product Tracking Data, User Movement Tracking Data

Patient Registries: An observational trial of patients sharing a common characteristic e.g. disease, that collects specific data over time on outcomes of interest. These may be held by specialist patient groups or advocacy organizations

Patient Testimonials: Information about a particular disease or therapy area and what it is like to live with that condition provided directly by a patient; can be in video, photo, text format

Pharmacy Order Messaging: Data related to the messages sent between a provider and a pharmacy to input orders

Examples: Data and Time of Message; Receiving Facility; Sending Facility; Patient Name, Date of Birth, Sex, Address, SSN; Order Status; RX Type; Order Number

Population-Level Health Outcomes: A measurement of the state of wellbeing a group of individuals at the aggregate level and the distribution of outcomes within the group

Examples: Mortality Rate, Morbidity, Life Expectancy, Condition-Specific Life Expectancy, Premature Death Rates, Disability-Adjusted Life Years (DALYs), Quality-Adjusted Life Years (QALYs)

Prescription Data and Adherence Data: Data relating to the details of a product or device prescription to a specific individual.

Examples: Past and Current Prescriptions, Patient Persistency

Product Identifying Data: Data which can be used, on its own, to identify the specific product, device, app, or cloud server an individual utilizes.

Examples: Product ID, Device ID, IP Address, OEM, Chipset, Hardware, Software

Product Preference Setting Data: Data provided through explicit feedback or extrapolated from individual settings on a product or device.

Examples: Dose settings, Push Notifications Status, Auto Download Updates

Product Service, Malfunction & Diagnostic Data: User provided data (or authorized passive data collection) allowing developer to interact with device/server/app to fix problems, troubleshoot, update software, and dialogue with customer

Examples: From User or Device - Service Calls, Performance/Malfunction Data

Product Usage Data: Data provided or captured about the individual's interaction with the service or product or device by the service provider.

Examples: Frequency, Amount, Nature of Use of Product

Product/Device Generated Data: Data collected by the product or device (entailing medical measurements such as heartrate or insulin levels, or entire categories of data, such as geolocation, dependent on type of device)

Examples: Heartrate, Steps Walked, Flights of Stairs Climbed, Blood Pressure, Frequency of Automatic Injections, Severity of Episodes

Personal Information/Data: A defined term under privacy and data protection laws to refer to data that is identifiable in some manner to a person. The GDPR uses “Personal Data,” referring to any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. The CCPA uses “Personal Information,” referring to Information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.³²

Protected Health Information (PHI): A defined term under HIPAA, referring to a subset of Individually Identifiable Health Information (IIHI), and basically means any information, whether oral or recorded in any form or medium, that is transmitted or maintained by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse in any form or medium and that relates to the past, present, or future physical or mental health or condition of an identifiable individual; the provision of health care to an individual; or the payment for the provision of health care for an individual³³

³²GDPR, Art. 4(1); The CCPA defines personal information as: “Information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following:

- (A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers.
- (B) Any categories of personal information described in subdivision (e) of Section 1798.80.
- (C) Characteristics of protected classifications under California or federal law.
- (D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
- (E) Biometric information.
- (F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer’s interaction with an Internet Web site, application, or advertisement.
- (G) Geolocation data.
- (H) Audio, electronic, visual, thermal, olfactory, or similar information.
- (I) Professional or employment-related information.
- (J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).
- (K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer’s preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.”

See: Cal. Civ. Code § 1798.140(o).

³³ 45 C.F.R. 160.103

Examples: Medial Record, Laboratory Report, Hospital Bill

Referral Data: Data related the diagnoses, procedures, hospital recipient, physician recipient that a physician refers for their patient as well as the reason, status, and priority of such referrals

Research Data from 3rd party: Specific data collected by a 3rd party based on an individual's interaction with products, services, or devices monitored by the 3rd party.

Examples: Census Data, TV Rating Data, Weather Data

Scheduling Data: Data related to the timing of patient appointments, treatment, care, and procedures

Examples: Number of Patients Seen, Fill Rates, Available Appointment Slots, Missed Appointments

Search Requests and Query Data: List of queries entered by the end user into the product, device, or service

Examples: Searches Within Apps, Internet Searches on Browser-Specific Pages, or Within Specific Web-Apps

Sexuality Data: Information about an individual's personal sex life or sexual orientation/identity

Examples: Sexual History, Sexual Health, List of Sexual Partners, Sexual Orientation/Identity, STIs

Social Interaction Data: Interactions between an individual and other users of services or apps

Examples: Individuals with Whom Individual Plays Online Games, Individuals from Whom Individual Receives "Invites" Through Server-Specific Calendar, Businesses with which Individual Interacts

Social Media Data: Information that users on social media website or applications share including text, video, and/or photo content, and its metadata

Examples: Blogs, Tweets, Facebook Posts, Instagram Posts, YouTube Videos, Flickr, LinkedIn Posts, Shares, Likes, Mentions, Hashtag Usage, Comments, URL Clicks

Substance Abuse/Use Disorder Data: Data related to a patient's substance use, addictions, diagnosis, treatment, or services

Examples: Addiction Data, Pattern of Abuse Data, Testing Results, Substance Abuse Facilities Data

Surveillance Data: Data systematically collected (active or passively) by government entities and typically related to diseases or conditions that may affect public health

Supply Order Data: Data related to the order of medical and surgical supplies

Examples: Item Types, Order Quantity, Delivery Times, Date, Total Value, Unit Price

Telehealth Data: Data generated from the use of electronic information and communications technologies to support long-distance the diagnosis, consultation, treatment, education, care, and management of a patient's healthcare, transmitted from a patient to a provider³⁴

Examples: Audio, Video, and Medical Data from Remote Patient Monitoring Devices

Transaction Data: Data chronicling financial transactions, interactions and activity of individual

Examples: Orders, Order History, Fulfillment Activity

Unique Identifier: A numeric or alphanumeric value that is associated with and references a specific, single information object within a system³⁵

User Stored Content: Record of input data provided by user through typing, verbal note-taking, or other document storage methods

Examples: Word Docs, Excel Spreadsheets, Pics, Communications Content

³⁴ "Telehealth Programs." Health Resources & Services Administration (2015), available at <https://www.hrsa.gov/rural-health/telehealth/index.html>.

³⁵ The CCPA defines unique identifier as: "A persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device. For purposes of this subdivision, "family" means a custodial parent or guardian and any minor children over which the parent or guardian has custody." See: Cal. Civ. Code § 1798.140(x).

Data Uses and Purposes

Adverse Event Reporting: The acknowledgement of any untoward medical occurrence in a patient, such as any unfavorable and unintended sign (e.g. an abnormal laboratory finding), symptom, or disease temporally associated with the use of a product³⁶

Authentication: The process by which an entity determines whether another entity is who it claims to be

Blocking and Logging: Refers to security technology/platform that is capable of blocking malicious access/activities and log critical information on access and key activities as an audit trail

Breach Notification: The notification of regulators and/or victims when the security or privacy of personal data has been compromised

Commercial Purposes: Any use directly or indirectly in connection with a business or for financial gain³⁷

Contextual Advertising: The delivery of messages and product offerings to a user based on a single visit to a web page, the content or theme of the web page, or a single search query; advertisements can be displayed that are not “targeted” to the person

Coordination of Benefits: The determination of payment responsibilities for plans that provide health and/or prescription coverage for a person with Medicare

Credentialing: The process of evaluating and establishing the qualifications and practice of licensed medical professionals through the review of education, training, residency, licenses, and certifications

Device Provisioning: The process of attaching a certificate or verification to the Company-owned device identity

³⁶ Food and Drug Association, “Guidance for Industry and Investigators – Safety Reporting Requirements for INDs and BA/BE Studies”, available at <https://www.fda.gov/downloads/Drugs/Guidances/UCM227351.pdf>

³⁷ The CCPA defines commercial purpose as: “[a purpose] to advance a person’s commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction. “Commercial purposes” do not include for the purpose of engaging in speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism.” See: Cal. Civ. Code § 1798.140(f).

Diagnosis: The determination of the nature of a medical condition present or absent in a patient

Eligibility for a Health Plan: The process of determining whether an individual has met certain conditions to be considered authorized for insurance coverage; Eligibility factors include: age, residency, citizenship, disability, certain conditions/diseases

Enrollment/Disenrollment in a Health Plan: The transmission of subscriber enrollment information from the sponsor of the insurance coverage, benefits, or policy to a health plan to establish or terminate insurance coverage

Health Care Claim Status Request and Response: The process of determining the status of a claim previously submitted to a health plan, typically used by providers

Health Care Electronic Funds Transfer: The messaging used by health plans to order a financial institution to electronically transfer funds to a provider to pay for healthcare services

Healthcare Operations: The administrative, financial, legal, and quality improvement activities necessary to run a healthcare business and support treatment and payment

Examples: Case Management, Care Coordination

Health Care Services Notification and Acknowledgment: The process of informing a health plan that an enrollee has undertaken health care services

Health Outcome: The analysis of the efficacy of a given treatment or therapy for a specific individual, often in consideration of the costs of the treatment/therapy, the safety and tolerability, and quality of life of the individual and often compared to the expected/desired outcome

Health Promotion: The process of empowering patients to increase control over their health and its determinants³⁸

Human Subject Research: Research that involves interactions with individuals or involves the processing of information that can be identified to an individual

Identity Management: Framework of policies and technologies for ensuring that the proper Company employees and contingent workers have the appropriate access to Company's technology resources and underlying data associated with such resources

³⁸ Sanjiv Kumar and GS Preetha, "Health Promotion: An Effective Tool for Global Health", 37(1) Indian J. Community Med. 5 (2012).

Interest-Based Advertising (IBA) /Online Behavioral Advertising (OBA):

Predicting preferences and showing advertisements based on interests known or inferred from data about a site user's visits over time and across websites or applications

Market Research: The systematic gathering and interpretation of information about individuals or organizations using the statistical and analytical methods and techniques of the applied social sciences to gain insight or support decision making; can include social and opinion research

Marketing: The process of communicating about, promoting, and/or advertising products or services with the intent to encourage the purchase or use of the product or service³⁹

Payment: A compensation made to an individual or other entity for services rendered or performed⁴⁰

Physical Securities Inspection: Internal investigation of Company incidents involving threats, violence, property damage, theft, and fraud

Prevention: The act of reducing the risk of developing disease or other morbidities and minimizing the burden of diseases and associated risk factors

Product Detailing: Interacting with a healthcare provider to provide information on a Company product or service. Covers both face to face promotion via sales force or providing information via other channels

Product Development: The process of producing new products or services, including activities that begin after "Research" when the creation of the idea or concept is first developed, the assessment of the feasibility of features of the product or service, the production of the product or service, and the introduction of the product into the market place.

Product Improvement: The process of enhancing or modifying existing products or services, seen as improvement to a version 1.1 or 2.0 of an original. Typically includes the analysis of the performance of an existing product, service, or feature; and/or the characteristics of a market or group of consumers to improve existing products. If

³⁹ HIPAA defines marketing as: "A communication about a product or service that encourages recipients of the communication to purchase or use the product or service." See: 45 C.F.R. 164.501.

⁴⁰ HIPAA defines payment as: "The activities of a healthcare entity to:
1) receive value, obtain payment or be reimbursed for their products or services,
2) obtain premiums to fulfill their coverage responsibilities and provide benefits under an insurance plan, and obtain or provide reimbursement for the provision of healthcare."
See: 45 C.F.R. §164.501.

product improvement indicates the need for another or different new product, the knowledge is shared with either product development or research entities to undertake new product development

Product Research: Research that is meant to develop a specific product and may begin to look like Product Development. Product Research may also be Human Subject Research.

Product Utilization Analysis: An analysis of the manner, timing, frequency, and indications for which a health care provider makes use of a given treatment or therapy. Almost always compared to an average or norm established by similarly situated entities. The goal of a product utilization analysis is to identify any over or under use of a product or therapy as compared to a normative value

Profiling: Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements⁴¹

Quality Assurance: The process of providing confidence that quality requirements will be fulfilled both internally to management and externally to users

Quality Control: The process of fulfilling quality requirements through inspection and analysis of product or service function

Recruitment of Clinical Trial Subjects: Identifying subjects who may meet the entry and exclusion criteria for a trial. Typically performed by site staff via medical notes review and/or on seeing a patient in clinic or by a third-party vendor by various methods. Third parties can be granted access to data mine GP and Health Institute records and alert them to potential clinical trial subjects or directly alert the patient to the existence of a trial in their area

Re-identification: The action of discerning the identities that have been removed from pseudonymized or de-identified data

⁴¹ The GDPR defines profiling as: "Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements." See: GDPR, Art. 4(4).

Research: A systematic investigation, including research development, testing and evaluation, designed to develop or contribute to knowledge of the researchers, the entity sponsoring the research, or to the generalizable knowledge of the public⁴²

Re-Targeting (Re-Marketing): The practice of collecting data about a visitor to one's own website or app and using it to target advertisements elsewhere on the internet to reach those same visitors; generally considered a subcategory of behavioral advertising

Sales: The delivery or other provision of a product or service to an individual in exchange for payment⁴³

Social Listening: The process of tracking and understanding digital conversations across the web about a particular phrase, word, or brand

Third-Party Vendor Invoicing: Suppliers submit invoices to Company to bill for goods and services provided. The invoice includes the amount to be paid, the terms of payment, and the remittance instructions

Treatment: The provision, coordination, or management of health care and related services for a specific individual⁴⁴

Treatment/Therapeutic Assessment: The analysis of the efficacy, safety, tolerability, compliance rate, etc., of a given treatment or therapy protocol generally within a population of patients

Visitor Management: A process of authorizing, identifying, and overseeing visitors at Company facilities

⁴² The Common Rule defines research as: "systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge. Activities which meet this definition constitute research for purposes of this policy, whether or not they are conducted or supported under a program which is considered research for other purposes." See: 45 C.F.R. §46.102(d); The CCPA defines research as: "Scientific, systematic study and observation, including basic research or applied research that is in the public interest and that adheres to all other applicable ethics and privacy laws or studies conducted in the public interest in the area of public health." See: Cal. Civ. Code § 1798.140(s).

⁴³ The CCPA defines sales as: "Selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration." See: Cal. Civ. Code § 1798.140(t)(1).

⁴⁴ US Department of Health and Human Services, "Guidance: Treatment, Payment, and Health Care Operations." HHS.gov. July 26, 2013. Accessed February 14, 2018. <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/disclosures-treatment-payment-health-care-operations/index.html>.

Actions Performed on Data

Aggregation: The compilation of raw data and its expression in a summary form for statistical analysis

Analytics: The use of mathematics, statistics, predictive modeling, machine learning, and other techniques to find meaningful patterns and knowledge in a dataset

Anonymization: A process of removing the association between the identifying dataset and the data subject by removing or manipulating direct and indirect identifiers with mathematical and technical guarantees to prevent re-identification⁴⁵

Artificial Intelligence (AI): A broad term used to describe the capability of computer processing systems to perform functions otherwise defined as those requiring human intelligence to accomplish

Automated Processing: The performance of operations upon personal information without any human intervention

Automatic Image Recognition: The use of computer programs to identify and detect objects or features in a digital image or video without the need for human intervention

Automatic Language Translation: The use of computer programs to convert one human language (speech or text) to another without the need for human intervention

Breach: The unauthorized acquisition, access, use, or disclosure of personal information which compromises the security or privacy of such information

De-Identification: The general term for any process that removes the association between a set of identifying data and the data subject by removing or manipulating direct and known indirect identifiers through manual or automated processes, or a combination of the two⁴⁶

⁴⁵ Simson L. Garfinkel, "De-Identification of Personal Information" (October 2015), available at <http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf>

⁴⁶ *Id.*; The CCPA defines deidentified info as: "Information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information:

- (1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.
- (2) Has implemented business processes that specifically prohibit reidentification of the information.

Deep Learning: A subset of machine learning that uses a collection or sequence of algorithms to model higher-level abstractions in data; based on neural network models with more than one hidden layer

Device Fingerprinting: The method of identifying visitors based on a combination of many different types of data that are automatically sent by a user's phone or browser, such as IP address, browser versions and plug-in details, system fonts, time zone, and other information

Encryption: The process of obscuring information, often by changing plaintext into ciphertext, to protect confidentiality of data as it is stored and transmitted by making information unreadable without special knowledge

Hashing: The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data⁴⁷

Machine Learning: A field of computer science which designs algorithmic based systems to learn from presented data rather than being explicitly programmed. A program or system that trains a predictive model from input data

Natural Language Processing (NLP): The analysis, manipulation, and/or understanding of human language (speech or text) by computers, typically accomplished through machine learning

Neural Networking: A variation of a machine learning model that, taking inspiration from the human brain, is composed of multiple processing layers

Processing: The performance of operations upon personal information that can include, but is not limited to, the collection, retention, logging, generation, transformation use, disclosure, transfer, and disposal of personal information⁴⁸

(3) Has implemented business processes to prevent inadvertent release of deidentified information.

(4) Makes no attempt to reidentify the information."

See: Cal. Civ. Code § 1798.140(h).

⁴⁷ Leighton Johnson, "Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response" (1st ed. 2013).

⁴⁸ The GDPR defines processing as: "Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." See: GDPR, Art. 4(2); The CCPA defines processing as: "Any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means." See: Cal. Civ. Code § 1798.140(q).

Pseudonymization: The replacement of names and other information that directly identifies an individual with pseudonyms in order to remove the association between identifying dataset and the data subject; indirect identifiers remain intact⁴⁹

Supervised Learning: Training a model from input data and its corresponding, previously assigned labels

Unsupervised Learning: Training a model to find patterns using an unlabeled data set

⁴⁹ The GDPR defines pseudonymization as: "The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person." See: GDPR, Art. 4(5); The CCPA defines pseudonymization as: "The processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer." See: Cal. Civ. Code § 1798.140(r).

