DEPARTMENT: Information Protection	**POLICY DESCRIPTION:** Patient Privacy Program Requirements
PAGE: 1 of 13	**REPLACES POLICY DATED:** 4/1/03, 2/1/06, 5/1/08, 9/23/09, 9/23/13, 3/1/14, 12/1/14, 9/1/17, 4/1/21
EFFECTIVE DATE: June 1, 2021	**REFERENCE NUMBER:** IP.PRI.001 (formerly HIM.PRI.001)
APPROVED BY: Ethics and Compliance Policy Committee	

SCOPE: All Company-affiliated facilities including, but not limited to, hospitals, ambulatory surgery centers, imaging and oncology centers, physician practices, shared services centers and corporate departments, Groups, Divisions and Markets.

PURPOSE: The purpose of this policy is to establish general requirements for the patient privacy program and provide pertinent definitions and provide guidance for some aspects of the Health Insurance Portability and Accountability Act (HIPAA) Standards for Privacy of Individually Identifiable Health Information (Privacy Standards), the Health Information Technology for Economic and Clinical Health Act (HITECH) component of the American Recovery and Reinvestment Act of 2009 (ARRA) and the Information Blocking restrictions set forth at 45 CFR Part 171 and issued pursuant to the 21st Century Cures Act.

To establish the requirements for each Company-affiliated facility to protect patients' privacy rights and their individually identifiable health information as required by the HIPAA Privacy Standards, 45 CFR Parts 160 and 164, and all Federal regulations and interpretive guidelines promulgated thereunder.

POLICY: All Company-affiliated facilities, primarily led by the Facility Privacy Official (FPO), must work to balance business needs and uses of protected health information (PHI) with patients' rights outlined in the HIPAA Privacy Standards. In addition to implementing the Company's patient privacy policies, each facility must develop and implement facility-specific policies regarding the privacy of, and access to, patient health information (see Attachment A for the minimally required policies).

Facilities in states with additional or more restrictive patient privacy requirements must develop and implement policies and procedures addressing the state-specific requirements.

Corporate departments, Group, Division and Market offices, ITG, HealthTrust/supply chain offices and shared services centers are business associates to each of the Company-affiliated facilities.

DEFINITIONS

The following definitions apply to all of the Company's patient privacy policies and procedures, and the facility sample policies and procedures.

Affiliated Covered Entity (ACE) – Legally separate covered entities that are affiliated may designate themselves as a single covered entity for the purposes of the HIPAA Privacy rule if each of the facilities is under common ownership or control.

DEPARTMENT: Information Protection	**POLICY DESCRIPTION:** Patient Privacy Program Requirements
PAGE: 2 of 13	**REPLACES POLICY DATED:** 4/1/03, 2/1/06, 5/1/08, 9/23/09, 9/23/13, 3/1/14, 12/1/14, 9/1/17, 4/1/21
EFFECTIVE DATE: June 1, 2021	**REFERENCE NUMBER:** IP.PRI.001 (formerly HIM.PRI.001)
APPROVED BY: Ethics and Compliance Policy Committee	

Audio Monitoring/Recording – For the purposes of this policy, "audio recording" refers to monitoring and/or recording an individual's voice using video cameras, cellular telephones, tape recorders, wearable technology (e.g., Google Glass), or other technologies capable of capturing audio or transmitting it for monitoring purposes.

Authorization – For purposes of this policy, "authorization" refers to a written form executed by the patient or the patient's personal representative that meets the requirements in the Authorization for Uses and Disclosures of Protected Health Information Policy, IP.PRI.010. Authorizations must be obtained for uses and/or disclosures of PHI that are not for treatment, payment, or health care operations purposes or are not otherwise permitted by the HIPAA Privacy Rule.

Breach – Any impermissible acquisition, access, use, or disclosure of unsecured PHI which compromises the security or privacy of such information.

Business Associate – A person, business or other entity who, on behalf of an organization covered by the regulations, creates, receives, maintains, or transmits PHI, including but not limited to claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and re-pricing; or provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person. A business associate is not someone in a facility's own workforce, such as an employee, volunteer, or trainee.

Civil Money Penalty (or Penalty) – The amount determined under 45 CFR 160.404, and includes the plural of these terms, imposed on a covered entity for violating an administrative simplification provision.

Community Clergy – Not a hospital employee, volunteer or workforce member; instead, they are a member of the clergy in the community at large.

Consent – For purposes of this policy, "consent" refers to the patient's or patient's personal representative's written acknowledgment and/or agreement of the use and/or disclosure of PHI for treatment, payment, or health operations purposes or other reasons permitted by the HIPAA Privacy Rule.

Continuity of Care Documents (CCD) – a core data set of the most relevant administrative, demographic, and clinical information facts about a patient's healthcare, covering one or more health encounters. CCDs are used to share data with providers and is one of the most commonly used methods for data exchange.

Correctional Institution – Any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. Other persons held in lawful custody includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial.

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 HIPAA.

Covered Functions – Those functions of a covered entity, including all business associate functions, the performance of which makes the entity a health plan, a health care provider, or a health care clearinghouse.

Covered Program – As described in the Standards for Confidentiality of Substance Use Disorder Patient Records Policy, BEH.001, a Covered Program is (a) an individual or entity (other than a general medical facility) who holds itself out as providing, and provides, substance use disorder diagnosis, treatment, or referral for treatment; or (b) an identified unit within a general medical facility that holds itself out as providing, and provides, substance use disorder diagnosis, treatment, or referral for treatment; or (c) medical personnel or other staff in a general medical facility whose primary function is the provision of substance use disorder diagnosis, treatment, or referral for treatment and who are identified as such providers. Covered Programs include, but are not limited to, those treatment or rehabilitation programs, employee assistance programs, programs within general hospitals, and private practitioners who hold themselves out as providing, and provide substance use disorder diagnosis, treatment, or referral for treatment who are treated as receiving direct or indirect federal assistance through Medicare participation, tax-exemption or other criteria as set forth in 42 CFR § 2.12. *See Standards for Confidentiality of Substance Use Disorder Patient Records Policy, BEH.001.*

Designated Record Set (DRS) – A group of records maintained by or for a facility that is the medical records and billing records about individuals maintained by or for a covered health care provider; the enrollment, payment, claims adjudication, and case or medical management record

systems maintained by or for a health plan; or used, in whole or in part, by or for the facility to make decisions about individuals.

Direct Treatment Relationship – A treatment relationship between an individual and a health care provider that is not an indirect treatment relationship.

Disclosure – The release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

Electronic Health Information (EHI) – Electronic protected health information as defined in 45 CFR 160.103 to the extent that it would be included in a designated record set as defined in 45 CFR 164.501, regardless of whether the group of records are used or maintained by or for a covered entity as defined in 45 CFR 160.103, but EHI shall not include: (1) psychotherapy notes as defined in 45 CFR 164.501; or (2) information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding. EHI excludes de-identification.

Note: Starting April 5, 2021, EHI is limited to and will be synonymous with the data elements represented in the United States Core Data for Interoperability (USCDI) v1 standard. On and after October 6, 2022, EHI constitutes the definition above. See Exhibit A, USCDI Data Elements, in IP.GEN.006, Information Blocking Rule Compliance Policy.

Electronic Media

1. Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card;
2. Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.

Family Member – with respect to an individual:

1. A dependent (as such term is defined in 45 CFR 144.103), of the individual; or
2. Any other person who is a first-degree, second-degree, third-degree, or fourth-degree relative of the individual or of a dependent of the individual. Relatives by affinity (such as by marriage or adoption) are treated the same as relatives by consanguinity (that is, relatives who share a common biological ancestor). In determining the degree of the relationship, relatives by less than full consanguinity (such as half-siblings, who share only one parent) are treated the same as relatives by full consanguinity (such as siblings who share both parents).
    i. First-degree relatives include parents, spouses, siblings, and children.

ii. Second-degree relatives include grandparents, grandchildren, aunts, uncles, nephews, and nieces.

iii. Third-degree relatives include great-grandparents, great-grandchildren, great aunts, great uncles, and first cousins.

iv. Fourth-degree relatives include great-great grandparents, great-great grandchildren, and children of first cousins.

Health Care – The care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following:

1. Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and
2. Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health Care Clearinghouse – An entity that processes health information received from another entity in a nonstandard format into a standard format or vice versa.

Health Care Operations (HCO) – See 45 CFR 164.501 for the specific definition. Includes any of the activities listed in Attachment B to the extent that the activities are related to covered functions which make the entity a health plan, health care provider, or health care clearinghouse.

Health Care Provider – A provider of services (as defined in Section 1861(u) of the Act, 42 U.S.C. 1395x(u)); a provider of medical or health services (as defined in section 1861(s) of Act, 42 U.S.C. 1395x(s)); and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Health Information – Any information, including genetic information, whether oral or recorded in any form or medium, that:
1. Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, 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.

Health Oversight Agency – A public agency authorized by law to oversee health care system or government programs where health information is necessary to determine eligibility or compliance or enforce civil rights laws (e.g., Federal Bureau of Investigation (FBI), U.S. Department of Health and Human Services (DHHS) Office of Inspector General (OIG), Office of Civil Rights (OCR)).

DEPARTMENT: Information Protection	**POLICY DESCRIPTION:** Patient Privacy Program Requirements
PAGE: 6 of 13	**REPLACES POLICY DATED:** 4/1/03, 2/1/06, 5/1/08, 9/23/09, 9/23/13, 3/1/14, 12/1/14, 9/1/17, 4/1/21
EFFECTIVE DATE: June 1, 2021	**REFERENCE NUMBER:** IP.PRI.001 (formerly HIM.PRI.001)
APPROVED BY: Ethics and Compliance Policy Committee	

Health Plan – An individual or group plan that provides, or pays the cost of medical care. Health plans include a group health plan, an HMO, Medicare Parts A and B, and Medicaid, among others. Examples of programs that are not health plans include workers' compensation, disability insurance, life insurance, automobile insurance, and coverage for on-site medical clinics. A complete listing of inclusions and exclusions is provided in the regulations.

Hybrid entity – A single legal entity that is a covered entity whose business activities include both covered and non-covered functions and that designates health care components and documents the designation.

Indirect Treatment Relationship – A relationship between an individual and a health care provider in which the health care provider:

1. Delivers health care to the individual based on the orders of another health care provider; and
2. Typically provides services or products, or reports the diagnosis or results associated with the health care directly to another health care provider, who provides the services or products or reports to the individual.

Information Blocking – means an act or omission ("Practice") that

(1) except as required by law or covered by an Information Blocking Exception, is likely to interfere with Access, Exchange, or Use of EHI; and

(2) if conducted by

(A) *a Health Care Provider*, such provider knows that such Practice is unreasonable and is likely to interfere with Access, Exchange or Use of EHI; or

(B) *a Health IT Developer of Certified Health IT or a HIN/HIE*, such developer or HIE/HIN knows, or should know, that such Practice is likely to Interfere with Access, Exchange or Use of EHI.

Information Blocking Exception – Even if a Practice may interfere with access, exchange, or use of EHI, it may still be permissible if it complies with one or more of the following eight exceptions:

1. Preventing Harm Exception
2. Privacy Exception
3. Security Exception
4. Infeasibility Exception
5. Health IT Performance Exception
6. Content and Manner Exception
7. Fees Exception
8. Licensing Exception

Refer to the Exception Review Team for guidance when considering these exceptions.

Law Enforcement Official – An officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:

1. Investigate or conduct an official inquiry into a potential violation of law; or
2. Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Organized Health Care Arrangement (OHCA) – This option, under the HIPAA Privacy Standards, allows the sharing of information for treatment, payment and health care operations between healthcare providers. The OHCA is defined as a clinically integrated care setting in which individuals typically receive health care from more than one health care provider. The U.S. Department of Health and Human Services (HHS) identifies the facility setting as "the most common example of this type of health care arrangement" because the facility and physicians with privileges at the facility "together provide treatment to the individual." HHS recognizes that the facility and its privileged physicians must be able to share information for treatment purposes and for their joint health care operations.

Payment – 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.

Personal Representatives – As specifically defined by state law, a person who has the authority to act on behalf of an individual in making decisions related to that individual's health care. Except as otherwise provided in 45 CFR 164.502(g) or elsewhere noted, when applying these privacy policies facilities must treat a patient's personal representative as the patient with respect to uses and disclosures of the patient's PHI, as well as the patient's privacy rights. Therefore, throughout these privacy policies, any reference to "patient" can be read to include the patient's personal representative unless otherwise excluded or noted.

Photography – For the purposes of this policy, "photography" refers to recording an individual's likeness (e.g., image, picture) using photography (e.g., cameras, cellular telephones), video recording (e.g., video cameras, cellular telephones), digital imaging (e.g., digital cameras, web cameras), wearable technology (e.g., Google Glass), or other technologies capable of capturing an image (e.g., Skype, fingerprint or iris scanning technologies). This does not include medical imaging such as MRIs, CTs, laparoscopy equipment, etc. or images of specimens.

Preparatory to Research Activity – Includes activities such as the writing of a research protocol, assessing feasibility of a written research protocol or verifying that an adequate population exists to conduct a protocol.

Prisoner (or Inmate) – A person that is incarcerated in or otherwise confined to a correctional facility.

Protected Health Information (PHI) – 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.

Protected health information 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.

Psychotherapy Notes – notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Qualified Protective Order – An order of the court or administrative tribunal or stipulation that prohibits the parties from using or disclosing the PHI for any purpose other than litigation or proceeding for which such information was requested and requires the return to the facility or destruction of the PHI at the end of the litigation or proceeding.

Record – Any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a facility.

Remuneration – Direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payment does not include any payment for treatment of an individual.

DEPARTMENT: Information Protection	**POLICY DESCRIPTION:** Patient Privacy Program Requirements
PAGE: 9 of 13	**REPLACES POLICY DATED:** 4/1/03, 2/1/06, 5/1/08, 9/23/09, 9/23/13, 3/1/14, 12/1/14, 9/1/17, 4/1/21
EFFECTIVE DATE: June 1, 2021	**REFERENCE NUMBER:** IP.PRI.001 (formerly HIM.PRI.001)
APPROVED BY: Ethics and Compliance Policy Committee	

Required by Law – A mandate contained in law that compels a covered entity to use or disclose PHI which is enforceable in a court of law. Required by law includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

Research – A systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge.

Sale of Protected Health Information – A disclosure of PHI by a covered entity or business associate, if applicable, where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI.

Sensitive Information – For purposes of this policy, sensitive information includes, but is not limited to, data which an external party shares ownership, rights or stakeholder interest or data with confidentiality requirements controlled by some regulating body, business unit, or contractual obligation (e.g., protected health information, social security numbers, employee human resources files) and restricted data (e.g., cardholder information, company passwords).

Staff Chaplains – Actual employees of the hospital or are hospital chaplain volunteers operating under the specific direction of a hospital employee (primarily the staff chaplain); thus, are actual workforce members.

Subcontractor – A person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.

Transaction – The transmission of information between two parties to carry out financial or administrative activities related to health care, including the following:

- Health care claims or equivalent encounter information
- Health care payment and remittance advice
- Coordination of benefits
- Health care claim status
- Enrollment and dis-enrollment in a health plan
- Eligibility for a health plan
- Health plan premium payments
- Referral certification and authorization
- First report of injury

- Health claims attachment
- Other transaction that the Secretary of HHS may prescribe by regulation

Treatment – 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.

United States Core Data for Interoperability (USCDI) - means the standardized set of health data classes and constituent data elements set forth at www.healthit.gov/USCDI.

Unsecured Protected Health Information – PHI that is not encrypted or rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary of HHS.

Use – With respect to individually identifiable health information, is the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

Video Monitoring – For the purposes of this policy, "video monitoring" refers to monitoring an individual or transmitting PHI or the patient's likeness using technologies capable of transmitting a video (e.g., video cameras, cellular telephones, web cameras, wearable technology) regardless of whether the transmission is recorded.

Violation (or Violate) – Failure to comply with an administrative simplification provision.

Workforce – Employees, volunteers, trainees, staff chaplains 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.

Additional Definitions – Please refer to the HIPAA Privacy Standards, 45 CFR Parts 160.101 and 164.501, for additional definitions.

PROCEDURE:

1. The facility, primarily led by the FPO, must maintain a Facility Privacy Program to include, but not limited, to:
   a. Implementation and compliance with all Company privacy policies and procedures (IP.PRI.001 - IP.PRI.013). When policies and procedures are revised, the previous versions of the policies and procedures must be retained for six (6) years.

b. Creation of, and revisions to, facility-specific policies and procedures (see Attachment A for the minimally required policies). When policies and procedures are revised, the previous versions of the policies and procedures must be retained for six (6) years.

c. Provision of education to all members of the facility workforce covering the HIPAA Privacy Rule and HITECH, Company privacy policies and procedures, and facility specific policies and procedures.
   i. Training for new workforce members must occur within a reasonable period of time (e.g., 30-45 days) after the person initially joins the workforce.

   ii. Any workforce member whose job function(s) is affected by a material change to a privacy policy and procedure must have training completed on the change within a reasonable period of time (e.g., 30-45 days) after such material change becomes effective.
   iii. Documentation of all workforce training, including sign-in sheets, dates, and topics covered, must be maintained for at least six (6) years.

d. Ensure appropriate administrative, technical, and physical safeguards are implemented and adhered to in order to protect health information from any intentional or unintentional use or disclosure that is in violation of privacy policies, the HIPAA Privacy Rule, or HITECH.

e. Identification of Business Associates – Company-affiliated facilities are required to have written agreements with their Business Associates.
   i. The FPO or designee at each facility must establish a process to identify its Business Associates.
   ii. Business Associate language must be added to existing contracts and be incorporated into new and renewing contracts, in consultation with the facility's legal operations counsel. See the Company's preferred Business Associate Agreement on the Atlas HIPAA Privacy site.
   iii. Corporate departments, Group, Division and Market offices, Corporate IT&S, and shared services centers are a business associate to each Company-affiliated facility.
   iv. As new regulations or laws are issued, Business Associate Agreement language must be revised.

f. Monitoring Program – The FPO must define and implement a process to routinely monitor compliance with the Company and facility specific policies and procedures, the HIPAA Privacy Standards, and HITECH that includes the following minimum requirements:
   i. The performance of privacy rounds (e.g., walking throughout the facility and interviewing workforce members to identify potential areas of noncompliance);
   ii. Auditing workforce members privacy training completion;

iii. In conjunction with the FISO, audit appropriate access to systems containing PHI; Documenting areas of noncompliance and creating a corrective action and follow-up plan; and

2. Reporting all monitoring findings to the committee charged with privacy oversight. Structural Options under the HIPAA Privacy Standards
   a. Affiliated Covered Entity (ACE) – Company-affiliated facilities that choose to designate themselves as an ACE must document the decision including a listing of each participating facility. The documentation must be maintained for at least 6 years from initial creation and 6 years from each modification.

   b. Organized Health Care Arrangement (OHCA) – A facility, physicians with privileges at that facility, and departments of the facility that are not owned or operated by the facility are all considered an OHCA. The OHCA enables the sharing of PHI without each covered entity providing its own Notice of Privacy Practices. The OHCA covers activities only at the integrated delivery setting. For example, physicians with staff privileges are part of the OHCA only when they are rendering care at the facility. The physicians' private offices are not part of the OHCA. (Physicians, therefore, in their private offices, must issue their own notice of privacy practices, obtain consent from their own patients, and develop and comply with their own policies and procedures.)

3. Personal Representatives – If a person has the authority to legally act on behalf of another (e.g., legal guardian) as defined by state law, that person must be treated as if he or she were the patient including the execution of all patient privacy rights (e.g., right to request access, amendment, restrictions, confidential communications, and receipt of the Notice of Privacy Practices).

4. Guidelines for Employment-related Testing and Assessment – Employment-related testing and assessments are created for and maintained by the Employee Health Department or Human Resources Department of the employing facility and are not used for any other purposes. As such, the HIPAA Privacy Standards do not apply.

5. Refraining from Retaliatory Acts – Company-affiliated facilities may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising any rights under the HIPAA Privacy Standards, or HITECH.

6. Substance Use Disorder Patient Information – Company-affiliated facilities must comply with any applicable standards under 42 CFR Part 2 and the Company's Standards for Confidentiality of Substance Use Disorder Patient Records Policy, BEH.001. If PHI involves Patient Identifying Information (as defined in the Standards for Confidentiality of Substance Use Disorder Patient Records Policy, BEH.001), facilities are directed to consult the Standards for Confidentiality of

DEPARTMENT: Information Protection	**POLICY DESCRIPTION:** Patient Privacy Program Requirements
PAGE: 13 of 13	**REPLACES POLICY DATED:** 4/1/03, 2/1/06, 5/1/08, 9/23/09, 9/23/13, 3/1/14, 12/1/14, 9/1/17, 4/1/21
EFFECTIVE DATE: June 1, 2021	**REFERENCE NUMBER:** IP.PRI.001 (formerly HIM.PRI.001)
APPROVED BY: Ethics and Compliance Policy Committee	

Substance Use Disorder Patient Records Policy, BEH.001, and must comply with that policy. If the Standards for Confidentiality of Substance Use Disorder Patient Records Policy, BEH.001, establishes different standards from those under other HIPAA policies relating to individuals who may sign an authorization, or other standards for access, uses or disclosures, where applicable, the facility should not use or disclose information except where permitted by both the Standards for Confidentiality of Substance Use Disorder Patient Records Policy, BEH.001 and other applicable policies.

REFERENCES:

1. Health Insurance Portability and Accountability Act (HIPAA), Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164
2. American Recovery and Reinvestment Act of 2009, Title XIII, Subtitle D
3. Privacy Official Policy, IP.PRI.002
4. Minimum Necessary Policy, IP.PRI.003
5. Patients' Right to Access Policy, IP.PRI.004
6. Patients' Right to Amend Policy, IP.PRI.005
7. Patients' Right to Request Privacy Restrictions Policy, IP.PRI.006
8. Notice of Privacy Practices Policy, IP.PRI.007
9. Patients' Right to Confidential Communications Policy, IP.PRI.008
10. Accounting of Disclosures Policy, IP.PRI.009
11. Authorization for Uses and Disclosures of Protected Health Information Policy, IP.PRI.010
12. Protected Health Information Breach Risk Assessment and Notification Policy, IP.PRI.011
13. Safeguarding Protected Health Information Policy, IP.PRI.012
14. Mitigating Inappropriate or Unauthorized Access, Use and/or Disclosure of Protected Health Information Policy, IP.PRI.013
15. Records Management Policy, EC.014
16. Business Associate Tools, available on the Company Intranet
17. Facility Model Policies are available on the Company Intranet
18. Standards for Confidentiality of Substance Use Disorder Patient Records Policy, BEH.001
19. Standards for Confidentiality of Substance Use Disorder Patient Records, 42 CFR Part 2
20. Information Blocking Rule Compliance Policy, IP.GEN.006

Minimally Required Policies

A list of required privacy policies can be found on Atlas Connect at:

- **http://connect.medcity.net/documents/56159066/64868636/Privacy+Policy+Master+List.docx/c921f5c9-cf4e-4cf0-9720-6243916f2ea7**

Health Care Operations (HCO) Definition with Examples

HCO 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).

Regulation inclusions	Facility Examples (not inclusive)
1. Conducting quality assessment and improvement activities Including outcomes evaluation and development of clinical guidelines, provided that obtaining generalizable knowledge is not the primary purpose of any studies resulting from these activities. Patient safety activities (as defined in 42 CFR 3.20): Efforts to improve patient safety and the quality of health care delivery; The collection and analysis of patient safety work product; The development and dissemination of information with respect to improving patient safety, such as recommendations, protocols, or information regarding best practices; The utilization of patient safety work product for the purposes of encouraging a culture of safety and of providing feedback and assistance to effectively minimize patient risk; The maintenance of procedures to preserve confidentiality with respect to patient safety work product; The provision of appropriate security measures with respect to patient safety work product; The utilization of qualified staff; and Activities related to the operation of a patient safety evaluation system and to the provision of feedback to participants in a patient safety evaluation system.	• Quality management activities such as performance improvement. • Risk Management Occurrence Reporting • Patient Access QA audits • Random charge integrity audits • Gallup surveys • ACoS Cancer registry • ORYX reporting • Case management • Utilization review • Letters sent to patients with new treatments that can be provided for specific diseases • Clinical Trials

Regulation inclusions	Facility Examples (not inclusive)
Population based activities relating to improving health or reducing health care costs Case management and care coordination Contacting of health care providers and patients with information about treatment alternatives Related functions that do not include treatment	
2. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance	• Peer review • Credentialing and Privileging Activities
Evaluating health plan performance	• Detailed analysis of A/R aging by payer
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	• Medical student training • Residency programs • Nursing / ancillary student training • Case conferences for residency program • Ongoing training for practitioners
Training of non-health care professionals	• HIM student training programs • Routine Education Department activities
Accreditation	• JCAHO
Certification	• State Agency surveys • HCFA surveys
Licensing Credentialing	• Physician credentialing
3. Underwriting, enrollment, premium rating and other activities relating to the creation, renewal or replacement of contract of health insurance or benefits	• Management of Employee Health Benefit Plans
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	• Would apply mainly to health plans

Regulation inclusions	Facility Examples (not inclusive)
4. Conducting or arranging or medical review, legal services and auditing functions including fraud and abuse detection and compliance programs	• Legal review • Internal Audit functions • HIM services audit functions • Risk Management Claims Management • Lab billing compliance audits
5. Business planning and development, such as cost management and planning-related analysis related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies	
6. Business management and general administrative activities of the entity including, but not limited to: • Management activities relating to implementation of and compliance with the requirements of this subchapter • Customer service, including the provision of data analysis for policy holders, plan sponsors and other customers, • Resolution of internal grievances, • Due diligence in connection with the sale or transfer of assets to a potential successor in interest, if the potential successor in interest is a covered entity or, following completion of sale or transfer will become a covered entity • Consistent with the applicable requirements of 164.514, creating de-identified health information, fundraising or the benefit of the covered entity, and marketing for which an individual authorization is not required as described in 164.514(e)(2).	• Patient Relations Program
	Auditing user access and resolution of HR disciplinary actions related to policy and procedure violation.