Policy Title: Protection of Confidential Information - Intermountain (Compliance)	
Effective Date: 08/28/2023	**Last Review Date:** 08/28/2023
Document Owner: Katie Gorris (Compliance and Ethics Director II)	**Next Review Date:** 08/27/2026
Approver: Suzie Draper (Business Ethics and Compliance VP)	

Purpose:

To provide guidance to Intermountain Health and its affiliated entities regarding each Workforce Member's, Medical Staff Member's, Organized Health Care Arrangement (OHCA) member's, Business Associate's, and research investigator's responsibility to protect Confidential Information, including Protected Health Information (PHI), when accessing, using or disclosing it, and to require such individuals to sign a standard Access and Confidentiality Agreement prior to accessing Confidential Information in any form including oral, written and/or electronic mediums. Refer to the Access and Confidentiality Agreement (ACA) - Intermountain (Compliance) - Supporting Document.

Scope:

Subcategories of DepartmentJobTitle not selected.

Entity Type(s):

Subcategories of DepartmentJobTitle not selected.

Definitions:

Access and Confidentiality Agreement (ACA) — A non-negotiable, confidentiality agreement between Intermountain Health and a User who will be granted access to an Intermountain Health electronic system or facility and performs functions or activities on behalf of, or provides certain services to, Intermountain Health regarding the protection of Confidential Information, including PHI, from unauthorized disclosure. The ACA may also be used to set expectations on confidentiality of Intermountain Health information with other authorized persons who use Intermountain Health's electronic resources (Resource Users) and/or have access to other Intermountain Health information. These obligations support federal and state regulations governing confidentiality and security, including the HIPAA Privacy and Security Rules.

Business Associate — An individual or entity, who is not part of a Covered Entity's Workforce, that creates, receives, maintains, or transmits PHI to provide a service on behalf of the Covered Entity or an Organized Health Care Arrangement (OHCA) in which the Covered Entity participates. Business Associate includes a subcontractor that creates, receives, maintains, or transmits PHI on behalf of the Covered Entity.

Confidential Information — Data proprietary to Intermountain Health, other companies, or other persons, plus any other information that is private and sensitive, and which Intermountain Health has a duty to protect. Confidential Information may be in any form including oral, written, and/or electronic mediums. Examples of Confidential Information include the following information that is maintained by, or obtained from, Intermountain Health:

- An individual's demographic, employment, or health information (including Protected Health Information and Personally Identifiable Information);
- Personnel and health plan information;

- Peer-review information;
- Intellectual property prepared or created by all persons working for or on behalf of Intermountain Health during the course of his/her employment or engagement;
- Intermountain Health's business information, (e.g., financial and statistical records, strategic plans, internal reports, memos, contracts, peer review information, communications, proprietary computer programs, source code, proprietary technology, etc.); and
- Intermountain Health's or a third-party's information (e.g., computer programs, client and vendor proprietary information, source code, proprietary technology, etc.).

Covered Entity — A health care provider, health plan, or clearinghouse that transmits any health information in electronic form in connection with a health care transaction and meets conditions of 45 CFR 160.103. A business associate is also a covered entity for certain standards, requirements, and specifications of HIPAA.

Disclose or Disclosure — With respect to PHI, the release, transfer, provision of access to, revealing in any other manner, information to any person or entity outside of Intermountain Health.

Organized Health Care Arrangement (OHCA) — A healthcare setting in which individuals receive healthcare services from more than one healthcare provider or a healthcare system in which more than one Covered Entity participates and takes part in at least one of the following joint activities: utilization review, quality assessment, or payment activities, expresses to the public that they are participating in a joint arrangement, and certain group health plans. The term is further defined in the HIPAA Privacy Rule.

Personally Identifiable Information (PII) — Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, or employment information.

Protected Health Information (PHI) — Individually identifiable health information (including demographic information collected from an individual and genetic information), transmitted or maintained in any form or medium that is created or received by or on behalf of a health care provider, health plan or healthcare clearinghouse, and which relates to the past, present or future physical or mental health or condition of an individual or the payment of healthcare for the individual, or provision of health care to an individual. PHI contains any of the individual identifiers at §164.514(b) of the HIPAA privacy regulations. PHI does not include education records, employment records, or records on individuals who have been deceased more than 50 years.

Resource Users — Any person, including Intermountain Health caregivers, contractors, consultants, interns/apprentices, students, affiliated physicians, fellows, temporary caregivers, etc., who use Intermountain Health resources and/or have access to Intermountain Health Information.

Use or Uses — With respect to PHI, the sharing, employment, application, utilization, examination, or analysis of information by any person working for or within Intermountain Health.

Users — Collectively, all Intermountain Health Workforce Members (including volunteers, residents, students, and fellows), Medical Staff Members, Select Health Providers, OHCA members, Business Associates, and research investigators.

Workforce or Workforce Member — Shall include, but not be limited to, Intermountain Health caregivers (including employed providers), volunteers, trainees, locum tenens, students, interns, residents, fellows, agency and traveling nurses, temporary service employees, individual contracted

staff, and other persons whose conduct, in the performance of work for Intermountain Health, is under the direct control of Intermountain Health as they perform their work, whether or not they are paid by Intermountain Health. Business Associates, with whom Intermountain Health has a Business Associate Agreement, are excluded from this definition.

Policy:

1. Protection of Confidential Information
    a. Every Intermountain Health Workforce Member, Medical Staff Member, OHCA member, Business Associate, research investigator, and Resource User is required to protect Confidential Information, including PHI, and abide by applicable confidentiality laws, regulations, bylaws, policies, and procedures.
        i. The Intermountain Health ACA establishes specific responsibilities Workforce Members, Medical Staff Members, OHCA members, Business Associates, and research investigators have in relation to the protection of Confidential Information, including PHI, from unauthorized disclosure. These responsibilities support federal regulations governing confidentiality and security, including the HIPAA Privacy and Security Rules.
        ii. All Workforce Members, OHCA members, Business Associates, research investigators, and Resource User who are granted access to Intermountain Health PHI or other Confidential Information shall acknowledge their responsibility to protect Confidential Information and PHI by signing the ACA. Workforce Members will be asked to agree to the terms upon hire or beginning of relationship, upon subsequent password changes for electronic use, at least every three years for non-electronic access, or when significant revisions to the ACA are made.
        iii. All members of the Medical Staff of an Intermountain Health facility or contracted providers at Medical Group clinics shall acknowledge their responsibility to protect Confidential Information including PHI by signing the ACA. Medical Staff members will be asked to agree to the terms upon initial credentialing and at the time of re-appointment. Medical Group contracted providers will be asked to agree at the start of their written agreement at least every three years or when significant revisions to the provider contract or ACA are made.
2. Use and Release of Confidential Information
    a. Workforce Members may use and release Confidential Information but only in compliance with Intermountain Health policies and procedures and job responsibilities. Release of PHI shall be subject to the [PHI Disclosure policies] [Use-Disclosure of PHI without Patient Authorization policy].
    b. This policy is not intended to limit access to or disclosure of confidential employee information in personnel records to persons who have a legitimate business reason to know of such information. This policy is also not intended to prevent employees from discussing their terms and conditions of work with coworkers or other individuals.
    c. All inquiries from the media, whether concerning Confidential Information or PHI shall be referred to the Communications Department or administration.
3. Misuse of Confidential Information
    a. Workforce Members who misuse Confidential Information will be subject to corrective action and other relevant legal remedies.

b. Workforce Members are required to report inappropriate use or disclosure of Confidential Information to their supervisor or director, Compliance, Legal, or Human Resources.

c. Other non-employed Users and Resource Users who misuse Confidential Information may be subject to loss of access to Intermountain Health resources and systems and legal liability, as applicable.

4. Confidentiality Orientation and Training

a. Employed Workforce Members

i. Orientation and training shall include material on how to protect Confidential Information including PHI and PII during the course of employment as well as their responsibility to continue to protect it after termination.

b. Non-Employed Workforce Members

i. The appropriate administrator or designee shall explain and distribute the ACA to non-employed Workforce Members (including volunteers, residents, students, and fellows) whose role relates to access, Use or Disclosure of Confidential Information or PHI.

c. Medical Staff Members and Contracted Providers

i. Medical Staff and contracted provider training shall include material on how to protect Confidential Information including PHI.

Procedure: Obtain Access and Confidentiality Agreements from Users and Resource Users - Intermountain

#	**Required Action Steps** (step by step process)	**Performed By**	**Supplemental Guidance**
1	Distribute ACA to all Users and Resource Users	DTS Identity Access Management Workforce Members Business Area Sponsors, Supervisors, Managers and Others in Workforce Member's Chain of Command	Distribution will be accomplished through Intermountain Health's master electronic account system for all Users and Resource Users, with limited exceptions. For Users that may not have electronic access to Confidential Information (such as volunteers, students, etc.), a sponsor over the business area, supervisor or above shall obtain individual's signed ACA in hard copy.
2	Review and agree to abide by the terms of the ACA.	All Users and Resource Users	The ACA shall be completed by Users and Resource Users through Intermountain Health's electronic systems upon first use or subsequent password changes, or in hard copy by those without electronic access. If obtained in hard copy, the individual's sponsor or manager shall retain a copy

			of such document through the term of employment or engagement and for three years after termination.

Procedure: Obtain Access and Confidentiality Agreements from Medical Staff Members or Contracted Providers - Intermountain

#	**Required Action Steps** (step by step process)	**Performed By**	**Supplemental Guidance**
1	Distribute ACA to all Medical Staff Members and Contracted Providers.	DTS Identity Access Management Workforce Members	Distribution will be accomplished through Intermountain Health's electronic systems upon first use and subsequent password changes. Access and ACAs may be tied to the credentialing and re-credentialing process for members of the Medical Staff. Signed agreements will be obtained electronically from contracted Medical Group providers upon first use and subsequent password changes.
2	Review and agree to abide by the terms of the ACA.	All Medical Staff Members and Contracted Providers	The ACA shall be electronically signed as part of the credentialing/re-credentialing process or onboarding process for Medical Group contracted providers or in hard copy by those without electronic access.
3	Maintain copies of ACAs agreed to by Medical Staff Members and Contracted Providers.	DTS Identity Access Management, Workforce Members	The ACAs shall be maintained in DTS electronic systems. If obtained in hard copy, the Medical Staff Office or the provider's manager shall retain a copy of such document through the term of engagement and for three years after termination.

References and/or Primary Sources:

- CFR 485.713 Condition of Participation: Physical Therapy Services
- CFR 485.721 Standard Protection of Clinical Record Information

Related Policies and/or Guidelines:

Legacy Intermountain Health

- Intellectual Property Policy
- Intellectual Property Distribution Policy

- PHI Disclosure Treatment Payment Operations Policy
- PHI Safeguards Policy
- Privacy Information Security Violation Sanctions

Legacy SCL Health

None

Supporting Documents:

- Access and Confidentiality Agreement (ACA) - Intermountain (Compliance) - Supporting Document