POLICY CLASSIFICATION: TMC Health	POLICY TYPE: Corporate Compliance - HIPAA	PAGE: **1** of **12**
DOCUMENT ID: CC-02-07	VERSION: F	EFFECTIVE: 10/14/2024
TITLE: **Identifying and Protecting PHI**		

Purpose:	This document describes the circumstances under which TMC Health (TMCH) identifies, treats, and handles Protected Health Information (PHI).
Definitions:	Access: The ability or the means necessary to search, view, read, write, modify, or otherwise interact with data or information contained in a patient's medical record. Access includes activity recorded in such a way that the time reviewed, time edited, and content reviewed, added, edited, or modified is recorded as part of an access log. Authorization: Permission from the patient or patient's legally authorized representative to use or disclose protected health information to an individual or entity for purposes other than treatment, payment, healthcare operations, or those allowed by law. Covered Entity: Health plans, health care clearinghouses, or health care providers who electronically transmit any health information in connection with transactions for which the Department of Health and Human Services (HHS) has adopted standards. Protected Health Information (PHI): Any information, including payment information, whether oral or recorded, transmitted or retained in any form or medium, including demographic information collected from an individual, that: • Is created or received by TMCH; • 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 • Identifies the individual, or with respect to which there is reasonable basis to believe the information can be used to identify the individual. Workforce Member: Employees, volunteers, trainees or other persons whose conduct is under the direct control of TMCH, whether or not the person is paid by TMCH.
Keywords:	Authorization, Email, Facsimile, Fax, HIPAA, PHI, Revocation, Verification

Applicability:	TMC Health: TMC Hospital Main and TMC Hospital at Rincon, including all inpatient and outpatient departments, Peppi's House – TMC Hospice, TMC Integrative Pain Clinic, and TMC Wound Care Center; TMC Medical Network and TMCOne, including all ambulatory primary and specialty care clinics, TMC Urgent Care – Rincon, and TMC Urgent Care – Wyatt; Benson Hospital, including Benson Hospital Rehabilitation, Benson Family Health Care Clinic, Benson San Pedro Clinic, and Vail Valley Family HealthCare; Northern Cochise Community Hospital, including Sulphur Springs Medical Center and Sunsites Medical Clinic; and all other TMC HealthCare subsidiaries except as otherwise noted. For purposes of this Policy, Affiliates do not include Tucson4Health LLC, Southern Arizona Hospital Alliance or TMCH joint ventures with physicians.
Statement of Policy:	**1. Identifying PHI** 1.1. Workforce Members treat information meeting the following criteria as PHI: (a) The information is created or received by a health care provider, health plan, employer, or health care clearinghouse; (b) The information 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; and (c) The information identifies the individual or there is a reasonable basis to believe the information can be used to identify the individual. 1.2. Workforce Members treat demographic information received by TMCH or disclosed to TMCH by another health care provider as PHI even if it does not include other information because it reveals that the individual received some type of care. **2. Patient Authorization** 2.1. *Obtaining Authorization* (a) Workforce Members do not require a patient to provide an authorization and will not condition treatment on obtaining an

authorization, except in the event (i) the patient is participating in research and the authorization is sought in connection with that research or (ii) the patient has requested an examination or other treatment in order to disclose that information to a third party, such as a request for an employment physical conducted for the purposes of giving that information to the patient's employer. In this case, Workforce Members may refuse to conduct the examination unless the patient signs an appropriate authorization form.

(b) For uses and disclosures of PHI requiring patient authorization (see TMCH policy **Use and Disclosure of PHI, CC-02-06)**, Workforce Members obtain patient authorization on a form containing the following:

- A specific and meaningful description of the PHI to be used or disclosed;
- The name of the person, organization, or class of persons or organizations that will be making the disclosure of PHI (e.g. Tucson Medical Center (TMC), TMCOne, Benson Hospital, Northern Cochise Community Hospital);
- The name or other identification of the person, organization, or class of persons or organizations to whom the PHI is being disclosed;
- A description of the purpose of the use or disclosure of PHI (if the patient has requested the disclosure, the description may be "at the request of the patient");
- An expiration date or an expiration event of the authorization that relates to the individual or the purpose or use of the disclosure;
- A statement that the patient has a right to revoke the authorization and a reference to TMCH's Notice of Privacy Practices for details to that right;
- A statement that TMCH cannot condition treatment on

whether the patient signed the authorization;

- A statement that the patient's PHI may be re-disclosed by the recipient and no longer be protected by federal privacy regulations;
- The patient's signature and the date of signature; and
- If the authorization is executed by a legally authorized representative, a description of that person's authority to act on behalf of the patient.

(c) If the patient signed an authorization, release, or other permission form before April 14, 2003, that does not comply with the authorization requirements set forth in this section, Workforce Members may continue to use or disclose the patient's PHI collected or received before April 14, 2003, following the terms of that previous authorization, release of other permission; however, to use or disclose PHI collected or received after April 14, 2003, from the same patient, a new patient authorization must be obtained that complies with the requirements of this section.

(d) If the patient signed an authorization form before September 23, 2013, that was HIPAA-compliant at the time of signature but that does not comply with all of the authorization requirements set forth in this section, Workforce Members may continue to use or disclose the patient's PHI collected or received before September 23, 2013, following the terms of that previous authorization; however, to use or disclose PHI collected or received after September 23, 2013, from the same patient, a new patient authorization must be obtained that complies with the requirements of this section.

(e) Workforce Members provide the patient with a copy of his or her signed authorization.

(f) TMCH retains copies of all patient authorizations for six years.

(g) TMCH retains copies of all patient authorizations in the patient's medical record.

2.2. *Utilizing Authorization*

(a) Workforce Members do not combine authorizations for different purposes with the single exception that, if the authorization is for the use and disclosure of PHI for treatment involved in a research study, the informed consent to participate in the study may be combined with the authorization to use and disclose the PHI for the same or another study; however, if TMCH conditions the provision of research-related treatment on one of the authorizations, any compound authorization created must clearly differentiate between the conditioned and unconditioned components and must provide the individual with an opportunity to opt into the research activities described in the unconditioned authorization.

(b) Workforce Members do not use or disclose PHI if the authorization is invalid. An authorization is invalid if:

- The authorization has expired because the expiration date has passed or the expiration event has occurred;
- The authorization form lacks a required element or has not been filled out completely with respect to a required element;
- TMCH is aware that the patient has revoked that authorization;
- TMCH knows that the form contains materially false information;
- The authorization is a conditional authorization and is not for the use and disclosure of PHI for treatment involved in a research study or for the use and disclosure of a patient requested examination or other treatment for the purposes of disclosing that information to a third party, such as a request for an employment physical conducted for the purposes of giving that information to the patient's employer; or
- The authorization is combined with another

authorization and is not for the use and disclosure of PHI for treatment involved in a research study, in which case the informed consent to participate in the study may be combined with the authorization to use and disclose the PHI for the same or another study. Note, if TMCH conditions the provision of research-related treatment on one of a combined set of authorizations, any compound authorization created must clearly differentiate between the conditioned and unconditioned components and must provide the individual with an opportunity to opt into the research activities described in the unconditioned authorization.

2.3. *Revocation of Authorization*

(a) A patient may revoke his or her authorization at any time by submitting a written request to the Health Information Management or Medical Records Department.

(b) Upon revocation of a patient's authorization, Workforce Members shall stop using or disclosing the patient's PHI for the purposes covered by the revoked authorization.

(c) TMCH retains copies of all patient revocations in the patient's medical record.

3. Verification of the Identity and Authority

3.1. A minimum of two patient identifiers must be verified whenever interacting with PHI. For example, at least two patient identifiers must be verified when entering PHI into the Electronic Medical Record (EMR) for registration, scheduling, arrival, insurance verification, and other data entry or verification activities.

3.2. A minimum of two patient identifiers must be verified prior to releasing PHI in any form, even when being released directly to the patient himself/herself.

3.3. Workforce Members take reasonable steps to verify the identity and authority of a person requesting PHI before disclosing the PHI to the requestor. Workforce Members document in the patient's medical record all steps taken to verify the identity and authority of

a person requesting PHI.

3.4. Workforce Members direct anyone whose identity and/or authority cannot be confirmed to the area supervisor or to the Health Information Management or Medical Records Department.

3.5. *Public Officials*

(a) Workforce Members request that a public official, or a person acting on behalf of a public official, complete the form **Verification of Identity and Authority of Government Official Requesting Access to Protected Health Information (MR-6740)** and present at least one of the following to verify his or her identity when requesting disclosure of a patient's PHI:

- If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of governmental status;
- If the request is made in writing, the request is on the appropriate government letterhead; or
- If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.
- A copy of the letter, ID badge, or other credentials shall be maintained in the patient's record, unless the person requesting the PHI completed the **Verification Statement** section of the form **Verification of Identity and Authority of Government Official Requesting Access to Protected Health Information (MR-6740)**.

3.6. *Patients*

(a) Workforce Members request a picture ID, such as a driver's license, from any patient requesting Access to his/her medical

records in order to verify his/her identity. A copy of the driver's license should be made and placed in the patient's record.

(b) If the request is received in writing, an attempt will be made to verify the signature of the patient with that contained in the record.

3.7. *Others*

When appropriate, Workforce Members ask any person requesting PHI to produce appropriate documentation to confirm his/her identity.

4. Exceptions to Verification of the Identity and Authority of a Requestor

4.1. If a Workforce Member knows the person requesting PHI, the Workforce Member is not required to verify identity and authority; however, the Workforce Member must document his/her knowledge of the person's identity and authority in the patient's medical record.

4.2. Workforce Members need not verify the identity and authority of a person requesting information from the patient directory (see TMCH policy **Use and Disclosure of PHI, CC-02-06**).

5. Methods to Verify the Identity and Authority of a Requestor

Workforce Members may use a variety of verification methods, always confirming a minimum of two identifiers, including but not limited to the following:

5.1. *Verification Methods for Requests Received via Telephone*

(a) Confirm the requestor's phone number with the information in the TMCH directory.

(b) Confirm the requestor's phone number with information from a prescription or order form.

(c) Confirm the requestor's phone number with the Professional

Services Directory.

(d) Confirm the information stated in the office greeting with information in the patient's record.

(e) Request that the caller identify him or herself and state his or her relationship to the patient.

(f) Request that the caller verify information detailed in the patient's face sheet.

5.2. *Visual Verification*

(a) Verify a patient's identity using a photo ID.

(b) Verify TMCH identification badges for all staff and providers.

(c) Verify identification badges of non-TMCH providers, insurance company representatives, or government representatives.

(d) Verify a requestor's identification with the requestor named on a written consent.

(e) Obtain vendor business cards and call the company to confirm, if necessary.

(f) Upon receiving a written request, verify signature with examples in the patient's chart.

(g) Obtain proof of government status, such as a badge, business card, appropriate government letterhead with a written request for PHI, a written statement on government letterhead that the person requesting the PHI is acting under the government's authority, a contract for services, a memorandum of understanding, or a purchase order.

5.3. *Oral Verification*

(a) Ask questions to verify face sheet or registration data, such as social security number, phone number, address, account numbers, etc.

(b) Ask the patient to confirm the role of the individual requesting

PHI.

(c) Ask the requestor to explain his/her relationship to the patient.

6. Safeguarding PHI

6.1. TMCH identifies and has in place appropriate administrative, physical, and technical safeguards in order to protect PHI from inappropriate and/or unauthorized Access, use, and disclosure.

6.2. Unauthorized individuals are strictly prohibited from entering any clinical or administrative work area. This includes, but is not limited to, patients, visitors, vendors, and any other persons who do not have authorization to be in these locations.

6.3. TMCH reasonably safeguards PHI from any intentional or unintentional use or disclosure that violates policy or law.

6.4. TMCH complies with the privacy and security standards for the electronic sharing of PHI pursuant to applicable law and regulations.

6.5. Workforce Members encrypt all emails containing PHI unless those emails are exclusively transmitted inside of a secure network, such as TMC's secure network. It is best practice to encrypt all emails containing PHI, regardless of the intention for the email to remain within a secure network. If no encryption technology is available for an email containing PHI outside of a secure network, Workforce Members are prohibited from sending PHI through email.

6.6. Smart phones and other wireless devices shall be enabled by the TMC I/S Department to Access TMC network email. The TMC I/S Department requires such devices to use adequate security measures to protect the confidentiality of PHI that may be Accessed or stored.

6.7. TMCH maintains policies, standards, guidance, and procedures outlining comprehensive administrative, physical, and technical safeguards for electronic PHI.

6.8. All facsimiles sent by or on behalf of TMCH are sent with a cover sheet containing a confidentiality statement that addresses the same

	or similar to the following: "The information contained in this facsimile message may contain patient health information protected under Federal and/or State Law and intended only for the use of the individual or entity named above. If the reader of this message is not the intended recipient, nor the employee, nor agent responsible for delivering it to the intended recipient, you are hereby notified that any dissemination, distribution, or copying of this communication is strictly prohibited. If you have received this communication in error, please notify us immediately by telephone and destroy the copy in your possession."
Procedure:	TMCH does not have a Procedure associated with this Policy.
Standard Work:	TMCH has not adopted Standard Work for this Policy.
References:	HIPAA Privacy Rule: §164.508 Uses and disclosures for which an authorization is required. January 25, 2013. HIPAA Privacy Rule: §164.514 Other requirements relating to uses and disclosures of protected health information. January 25, 2013. Rosati,K., & Owens, K. (2002). The Arizona HIPAA Privacy Toolkit for Hospitals, Compliance Guide. AZ: Coppersmith Gordon Schermer Owens & Nelson PLC.
Policy Creator:	TMCH Chief Compliance Officer
Executive Sponsor:	TMCH Chief Executive Officer
Review:	This Policy shall be reviewed as needed per changes in applicable laws, regulations, and accreditation or operational requirements, but no less often than every one (1) year.

Approved: /s/ Denise Hathaway 10/14/2024

Denise Hathaway
TMCH Chief Compliance Officer Date