

# HIPAA TRAINING JUNE



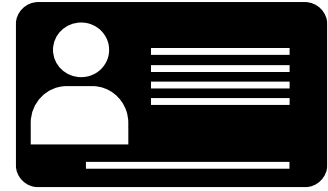
## HIPAA Form PF-7000

# “Verification of Patient Identity”

Argus

MEDICAL MANAGEMENT, LLC

The Physician Practice Management Company®



# Medical Identity Theft



**Medical identity theft** is when someone steals or uses a person's personal information (like name, Social Security number, or Medicare number), to submit fraudulent claims to Medicare and other health insurers without your authorization.

- **Medical identity theft can *disrupt a patient's medical care, and wastes taxpayer dollars.***
  - For example, in an emergency situation, a patient who has been incorrectly identified could be given a transfusion of the wrong blood type.
  - For example, a **thief** that uses personal information to see a doctor, get prescription drugs, buy **medical** devices, submit claims with your insurance provider.



MEDICAL MANAGEMENT, LLC

The Physician Practice Management Company®

# To verify a patient's identity, you can use a combination of methods, including:

- **Photo ID:** Ask for a valid government-issued photo ID, like a driver's license or passport.
- **Security Questions:** Ask for information like the patient's date of birth, address, phone number, **SSN** or medical record number.
- **Follow Up:** After a patient accesses their information, send a confirmation message via email or SMS.
- **Educate Patient:** Educate patients on the importance of correct identification while respecting their privacy.

*It's important to verify a patient's identity every time, and **use at least two identifiers.***

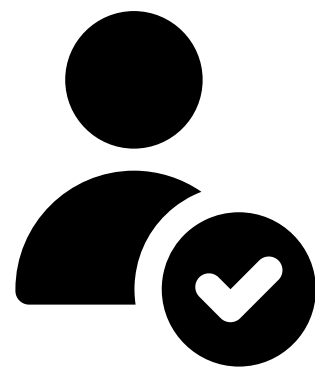


MEDICAL MANAGEMENT, LLC

The Physician Practice Management Company®



The way to **stop** medical **identity theft** and **identity confusion** is to *improve patient identification and provide enhanced data protection*



Form PF-7000  
HIPAA FORM FOR  
VERIFICATION OF IDENTITY



OFFICE NAME: \_\_\_\_\_

OFFICE ADDRESS: \_\_\_\_\_

PHYSICIAN NAME(S): \_\_\_\_\_

**VERIFICATION OF PATIENT IDENTIFICATION**

Name: \_\_\_\_\_ Document verifying name: \_\_\_\_\_  
*Document verifying name must not appear altered or forged*

Date of birth: \_\_\_\_\_ Document verifying DOB: \_\_\_\_\_  
*Document verifying DOB must not appear altered or forged*

S.S. #: \_\_\_\_\_ Document verifying SS#: \_\_\_\_\_  
*Document verifying SS# must not appear altered or forged*

California Drivers license # \_\_\_\_\_ Other State and # \_\_\_\_\_

Photograph copied to chart  Yes  No (if no, see below)  
*Patient must have photo identification or see below*

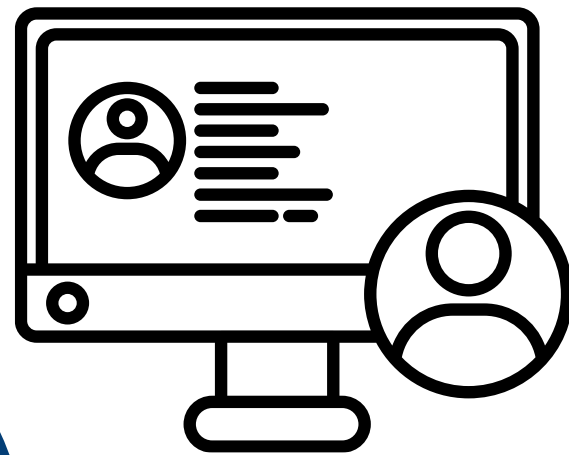
Physical Description entered in chart  Yes  No

**VERIFICATION OF PATIENT'S AUTHORIZED REPRESENTATIVE**

1. **Must have proof of authorization to receive information. Document should not appear forged, altered or destroyed and re-assembled. Verify patient signature.**
2. **Must have photo identification to verify their identity prior to release of information.**

# ***Verify the identity by scanning in the identity card and checking at visits.***

- Check that you got the whole facial image
- Keep the patient identity information secure



## RED FLAGS THAT MIGHT INDICATE IDENTITY THEFT

The FTC and other experts have identified examples of these warning signs, including:

1. Suspicious documents, such as a forged or altered driver's license or health insurance card.
2. Photographs or a physical description on file are not consistent with the appearance of the patient
3. A patient who has an insurance number but never produces a card or other documentation.
4. A query from a patient regarding a bill or insurance statement for services never received or in another individual's name.
5. Records showing medical treatment that is inconsistent with a patient's medical history.
6. A notice from a patient or law enforcement entity indicating possible identity theft.
7. Unusual billing patterns.
8. Other inconsistent information identifies the patient
9. Inconsistent signatures on file
10. Patient forms or applications appear forged, altered, or destroyed and reassembled
11. Statements sent to the patient or guarantor are returned as un-deliverable despite ongoing transactions on active records

A patient whose identity cannot be verified should not be seen until their identity can be verified. A long-time patient who has not exhibited any of the above listed "red flags" while receiving care in your office should not be turned away but any new staff who are not familiar with the patient should still verify the identity of the patient if existing staff who are certain of the patient's identity are not present. A patient who presents verification which meets any of the Red Flag criteria listed above should not be seen by the physician and should be reported to local law enforcement authorities and if the patient's information is already entered into Care Tracker a warning note should be posted for other offices to see.



MEDICAL MANAGEMENT, LLC

The Physician Practice Management Company®

A patient whose identity cannot be verified should not be seen until their identity can be verified.

A patient who **presents verification which meets any of the Red Flag criteria** listed on the previous slide ***should not be seen by the physician*** and should be reported to local law enforcement authorities.

- ***If the patient's information is already entered into Care Tracker, a warning note should be posted for other offices to see.***

