**TronsHealth**
5900 Balcones Drive STE 11857
Austin Texas 78731
Fax: (512) 485-2866

# TronsHealth

## §170.315(d)(12) Encrypt authentication credentials

**PREPARED FOR**

**ONC-ACB**
ONC Certification

**PREPARED DATE**
Aug 09, 2024



©2024 TronsHealth LLC, All Rights Reserved

## Table of Contents





©2024 TronsHealth LLC, All Rights Reserved

# 1. Overview

The Health IT Certification Criteria under §170.315(d)(12) require the encryption of authentication credentials to ensure the security and privacy of patient data within Health Information Technology (Health IT) systems. This requirement is from the Office of the National Coordinator for Health Information Technology (ONC), which has a noble mission to improve the security of electronic health information (EHI) by limiting unauthorized access.

Encryption of authentication credentials safeguards sensitive information, including passwords used to confirm a user's identity, against potential breaches and unauthorized access during transmission and storage.

# 2. Key Requirements

## 2.1 Encrypted Authentication Credentials

- Health IT developers must attest "yes" or "no" to whether their Health IT Module encrypts authentication credentials. The criterion does not mandate the inclusion of these encryption capabilities for any specific use case, nor does it require healthcare providers to implement these capabilities within their settings.
- If a health IT developer attests "no" to supporting encryption of stored authentication credentials, they must explain to the ONC Authorized Certification Body (ONC-ACB). This explanation must be submitted in hard copy or an acceptable human-readable electronic format.
- Health IT developers should ensure transparency by providing a hyperlink to any optional documentation related to their attestation. This link should be published with the product listing on the ONC Certified Health IT Product List (CHPL).
- Health IT developers are recommended to use the updated encryption standards documented by the National Institute of Standards and Technology (NIST). This includes using algorithms identified as approved security functions in the revised Federal Information Processing Standards (FIPS) Publication 140-2, dated October 12, 2021.
- Encryption of authentication credentials may involve password encryption or cryptographic hashing, where passwords are stored in encrypted form or as cryptographically hashed values, as referenced in 85 FR 25700.

### 2.1 Attesting "no"

- If a health IT developer attests "no" to supporting encryption of stored authentication credentials, they may explain why. For instance, the developer could state that their Health IT Module is not designed to store authentication credentials, so encryption of such credentials is not applicable.



©2024 TronsHealth LLC, All Rights Reserved

## 3. Importance

- Encrypting authentication credentials is crucial for safeguarding electronic health information (EHI) security and privacy within Health IT systems. This practice helps prevent unauthorized access by ensuring that sensitive information, such as passwords and authentication tokens, is protected during transmission and storage.
- By encrypting these credentials, Health IT systems reduce the risk of data breaches and unauthorized access, thereby maintaining the confidentiality and integrity of patient data.
- Compliance with this criterion also aligns with broader security standards and regulations, ensuring that Health IT products meet the requirements for protecting sensitive health information.

## 4. Implementation (Yes)

At TronsHealth, we prioritize the security of our users' credentials by implementing robust encryption measures that are in line with ONC standards. Specifically, we utilize the SHA-256 hashing algorithm to encrypt user passwords within our database. This advanced encryption method provides an important level of security by transforming passwords into a fixed-size hash, making it impossible for unauthorized parties to reverse-engineer the original password. By adopting SHA-256, we significantly reduce the risk of security breaches, ensuring that our users' sensitive information remains protected and secure.


©2024 TronsHealth LLC, All Rights Reserved