

Password policy

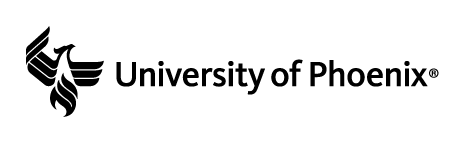
Mojo Software Solutions, Inc.



August 10, 2020

Shane Ẽire Byrne

CYB407



**Version:**

V1.016D August 10th, 2020; Approved by: S. E. Byrne

**Purpose:**

This policy prohibits the use, storage, and discloser of Personal Health Information (PHI) and Electronic Personal Heal information (EPHI) except as specifically permitted or required by HIPAA regulation.

**Scope:**

Any authorized access points to Mojo Software Solutions, Inc.’s network or cyber infrastructure, including but not limed to, Wi-Fi connection, ethernet connection, PAM, VPAM, VPN, Desktop Sharing, Network Access Control, Server access, Friendly Net Detection (FND), and any other means of connection. This policy is enforceable towards Mojo staff, vendors, and clientele who are applicable herein.

**Policy:**

1. PHI and/or ePHI shall be defined as any of the 18 distinct demographics that can be used to identify a patient. This includes name, address, dates (with the exception of years) which are directly related to an individual (birthday, admission/discharge date, date of death, or exact age of an individual), telephone number, fax number, e-mail address, Social Security Number (SSN), Medical record number, Health plan beneficiary number, Account number, Certificate/license number, Vehicle identifies, serial numbers, license plate numbers, device identifiers, Web Uniform Resource Locator (URL)’s, IP Addresses, Biometric identifiers (exempli gratia: fingerprint or voice print records), Full-face photos, and any other unique identifying numbers, characteristics, or codes. A password is a string of characters that is used to verify the identity of a user during an authentication process (exempli gratia: logging into one’s account). A strong password is defined as meeting the criteria of being eight characters or more, this in tern can be a collection of any non-repeating sequence of numbers, letters, of symbols (exempli gratia: !, @, #, $, %, and so on).
2. Upon being granted access to Mojo’s cyber infrastructure (id est: one’s login credentials) the user in question will be instructed by the system to generate a replacement password for the one issued to thus them by the IT department. The password policy of Mojo Software Solutions, Inc. is as follows: a strong password is to be required to be generated by the user, shall not contain any personal information of the user (exempli gratia: one’s name, user name, or company name), it must be unique from any other prior used passwords, and should have characters that are both uppercase, lowercase, numbers, as well as special characters as mentioned prior. It is also advisable to for a password to not host any correctly spelled words. Best practices for generation of a strong password are developing a passphrase based off something one is into, such as a recreational hobby as such. Hypothetically, say one is into basketball, a passphrase that could be generated from this is “IlikeBasketball!”, while this may fulfill the bottom-line expectations of a password, one can further secure their password through the concept of obscurification; this being the act of making something obscure. An example of this being taking the prior generated passphrase of “IlikeBasketball!” and substituting characters enough to the extent it makes it difficult to decipher the overall password itself. An example of this being “1Li|<3|3a$k3t|3@l1!”.
3. To keep passwords stored in the system secured they will be placed through a process known as an iteration count. The core concepts of an iteration count are the user provides their password. The system takes this and generates a random unique salt for the user and hashes the concatenation of both with a SHA-2. Salt is random data that is uses as an additional input to a one-way function that hashes data, a password, or passphrase; this will help safeguard the password while it is stored. A hash is a function that converts one value to another; within it is an algorithm that replaces characters of what is being hashed with other characters. Secure Hash Algorithm 2 or SHA-2 is a set of cryptographic functions that were designed by the United States National Security Agency (NSA) through the utilization of a block cypher. The system then takes the generated hash as discussed prior, concatenates it against the random salt generated and hashes it until a predetermined set of iterations are accomplished finally storing the result in a secured database.
4. The parties covered under this policy are as follows: any associate or agent of Mojo Software Solutions, Inc. which by their specific job function are allotted an approved means of access to Mojo’s systems through an approved channel (exempli gratia: computer terminal or portable terminal), any vendors deemed necessary to have access to Mojo’s systems through any such remote connection or approved device, and finally any clientele approved access to Mojo’s systems through either remote means or the use of approved devices to access said systems.
5. This policy herein will require any of the aforementioned parties to adhere to the password policy laid out. They will maintain access to Mojo’s systems on the basis of compliance with this password policy, knowing full well any misconduct may result in grievous actions being taken by Mojo Software Solutions, Inc. that may include fortification of any privileges granted to Mojo’s systems. In the case of an agent for Mojo Software Solutions, Inc. violation of this policy may result in formal declination up to and possibly including termination. For any vendor granted access, any violation of this policy may result in the immediate revocation of privileged access to Mojo’s systems, as well as the possible nullification of any business ventures with said vendor. In the event of clientele violating this policy, the immediate revocation of their privileged access to Mojo’s systems shall herein be forfeited.
6. This policy shall remain in accordance with NIST SP 800-63A, NIST SP 800-63B, and NIST SP 800-63C.

**References**

Bizmanualz, Inc. (2020) How to Write a Business Policy

Retrieved from

<https://www.bizmanualz.com/write-better-policies/how-to-write-a-business-policy.html>

Bluhm (March 27, 2019) NIST 800-63 Password Guidelines

Retrieved from <https://securityboulevard.com/2019/03/nist-800-63-password-guidelines/>

Compliancy Group LLC (2020) HIPAA Electronic Protected Health Information (ePHI)

Retrieved from <https://compliancy-group.com/hipaa-ephi-electronic-protected-health->

information/#:~:text=Electronic%20protected%20health%20information%20or,used%20

to%20identify%20a%20patient.

Conviso (14/01/2014) Wort and best practices for secure password storage

Retrieved from <https://blog.convisoappsec.com/en/worst-and-best-practices-for-secure-password-storage/>

Grassi, P., Fenton, J., Periener, R., Regenscheid, A., Burr, W., Richer, J. (June 2017)

NIST Special Publication 800-63B: Digital Identity Guidelines

Retrieved from <https://pages.nist.gov/800-63-3/sp800-63b.html>

Martins, F. (July 15, 2014) Creating Strong Password Policy Best Practices

Retrieved from <https://www.digicert.com/blog/creating-password-policy-best-practices/>

Rogers, B. E., Dunkerley, D. (2015). CRISC Certified in Risk and Information Systems Control

All-in-One Exam Guide. [[VitalSource Bookshelf version]].

Retrieved from vbk://1260118088

Rouse, M. (2020) Password

Retrieved from <https://searchsecurity.techtarget.com/definition/password>

Rouse, M. (2020) Salt

Retrived from <https://searchsecurity.techtarget.com/definition/salt>

TechTerms (April 21, 2018) Hash

Retrived from https://techterms.com/definition/hash#:~:text=A%20hash%20is%20a%20function,checksum%20generation%2C%20and%20data%20indexing.