

HIPPA Password and Security

HIPAA password requirements require effective structure and program. NIST (National Institute of Standards and Technology), is a federal regulatory body that gives security guidance on password creation to keep data safe.

- **Use of minimum of 8 characters**
- **Avoid password hints**
- **Create memorable passwords**

Admin/User Registration Form

[Home](#)

Please fill out the following form and press Register to register a new User. Enter permission level as number 0-4.

Username

pgrgdtl

Password

First name

Singh



Please match the requested format.

Password must contain at least one number, one uppercase, lowercase letter and 1 special character, and at least 8 or more characters

Last name

Our software program, COVID testing site, fulfills the requirements set by NIST. Our password requirements are it must be atleast 8 characters, 1 number must be used, 1 capital letter must be used and atleast 1 special character must be used, with the exception of semicolon. Also there are no hints given to the user. These password requirements guarantee complexity against hackers and also simplicity for in order the user to remember the password. Along with password requirements, we also have requirements for username. Allowing the user to have their own unique Password and Username allows for added protection on user medical information.

Admin/User Registration Form

[Home](#)

Please fill out the following form and press Register to register a new User. Enter permission level as number 0-4.

Username

pgrgdtl

Password

First name

Singh



Please match the requested format.

Only letters and numbers

Along with Password and Username requirements, our software also has email verification for when a user account has been created. "HIPAA does not prohibit the electronic transmission of PHI. Electronic communications, including email, are permitted". Our registration process includes sending an email to the user in order to verify their account.

Under HIPAA's security rule.

- Technical: These security standards address safeguards that must be in place to protect infrastructure that can access, handle, or store electronic protected health information (ePHI). Examples include having anti-virus software, data encryption, and firewalls.
- Administrative: These security standards address safeguards that must be in place to guide staff on the actions they should take to maintain the security and integrity of PHI. Examples include authorization of access to PHI, employee training, and password management.

Our software complies to these requirements with Bcrypt hashing of the user password and the user email. Bcrypt allows for user password to be stored in a slow hash with a salt in our table so that the program remains resistant to brute force search attacks. Referencing to HIPAA requirements, we have a way to encrypt passwords and emails that lead to electronic protected health information.

password

\$2y\$10\$khzwCTKaIXGfti0XYx5VkuWeZj2QDkLC4JV1Tm0fi72...

\$2y\$10\$CkBzcf5QHcf2/ZrXYfiNj.JH5cnq2MeQKomJxlgICcM...

\$2y\$10\$lex7HvEUoylIESDSzXfJXNupakumMUGFz8xQcGNsPtVo...

\$2y\$10\$r8dD1nNNeNhGmDcJZklrMumzeLfCljN/FHF5QOGFWRp...

\$2y\$10\$G31XsG/5TeqZBHNW/9DCL.I.wr8eWr2IHH4nYFDyemH...

\$2y\$10\$bohoM0ZIHyzUr1PlmClYeOVgU7d0jY8tEuKkLTKFGZK...

\$2y\$10\$ZpljSStCvqT0FVMTLSwsNOJLvVw/Nd9g2miV3fS7QY2...

\$2y\$10\$v.jhFJih0WtsCbuW94VRn.dL1CfV8H4yCnWyDjVevNM...

\$2y\$10\$mEbkr7ekRH4s9EFtq0yykO1NrVRQlkQoi6TFnHklZE8...

\$2y\$10\$zRprXP6cd8EL1Hb8jIWxeO9jiOZQCGzOK1F3L7/hsyq...

\$2y\$10\$Eb7oU1OcTb/GmYWEZAg/tO5w7WDQqYoKWFKmuzBjJb4.

\$2y\$10\$vUXkMvrtEnvw4lfwX0eUBO6GhbiHzlezOK1PL5qE9xd...

This encryption process of passwords and emails through Bcrypt along with the password requirements to make a password and username follow HIPAA compliance and allow for it to be a safe password storage.

Sources

<https://compliance-group.com/hipaa-password-requirements/>

<https://www.hipaajournal.com/hipaa-password-requirements/>

<https://www.hipaaguide.net/hipaa-password-requirements/>