Data Privacy & Security

The Seeker comes first above all else at **findhelp**. We're protective of Seekers' data and take extraordinary measures to secure their information. As such, we've developed multiple policies and procedures to ensure that the integrity of privacy is maintained throughout **findhelp's** Platform. We have solutions for role-based privacy, vulnerability management and system maintenance, as well as an Incident Response program as part of our broader Written Information Security Policy. Access to sensitive information is always limited to authorized and authenticated users, and our processes include user consent to determine access. We absolutely do not market to Seekers.

We follow the HITRUST CSF for its policies and procedures, which incorporates HIPAA as well as NIST 800-53 security controls. Protected information under HIPAA will not be shared with CBOs. Our customers follow their own policies when choosing to share protected information with CBOs as part of care coordination permitted by HIPAA. You may choose to share protected information (PII and PHI) within the **findhelp** Platform. We have robust employee security training, a vulnerability program with SLA's, and conduct risk analyses annually, as well as upon significant system changes.

How is seeker information collected and stored in findhelp?

Seeker information that is collected in **findhelp** is demographic information. This is used to uniquely identify seekers. Customers can set up additional features such as Assessments to collect additional actionable information about their seekers.

Seekers can use the **findhelp** platform directly and provide their own information, or Helpers can collect information on behalf of a Seeker.

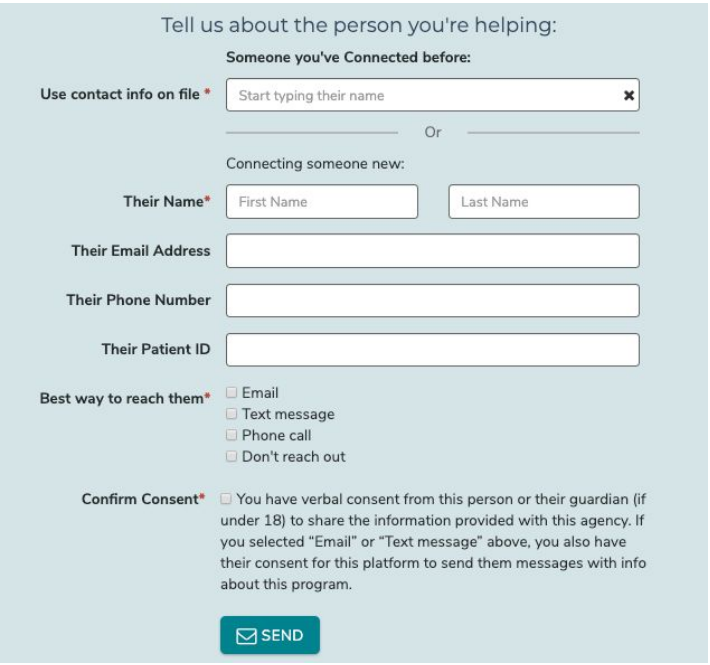
This information can be found in the Seeker Profile. From the People I'm Helping Dashboard, Helpers can select a person's "Seeker Profile," a page that brings together the different navigation activities the Helper, or their team, have taken on behalf of that Seeker. These navigation activities include referrals, goals, notes, and Assessment responses where applicable. Seeker Profiles are made by default any time a referral or Assessment is made by, or on behalf of, a Seeker.

Seeker Personal Information stores important personal information about the Seeker such as name, email address and phone number so that the Helper can easily view that information. Additional fields, such as Patient ID, address, or zip code can be added for Professional and Enterprise customers to track even more information. Information is stored securely and access to that information is controlled by the customer to protect the Seeker's Personally Identifiable Information (PII).

> *Seeker Profile Information is stored at the level of the White Label site, which means that when someone with Worker-level access on a White Label makes a referral or administers an assessment on behalf of a Seeker, they will gain access to view and update that Seeker's profile—which may include data previously saved by other workers on the site. Customers' compliance/legal teams may need to sign off on Custom Seeker Profile Fields to make sure that their policies comply with storage and access to that data.*

Referrals

A common way Seeker Profiles are created is automatically when a Referral is created. Below is what a Helper would see while collecting information to refer a seeker to a program:



This form includes fields for the seeker's name, e-mail address, phone number, patient ID (if applicable), contact type preference, and consent. Only name, contact preference, and consent are required. No clinical information is collected at any time.

The Seeker and the Helper have access to the information provided within the **findhelp** platform. Other Helpers at the organization may see this information as well if their user role is set up to do so with Team Navigation. The CBOs are able to see all of the Seekers who have been referred to their program, their contact information, and the best way to reach them. They will also see the name of the Helper (if applicable) and the date of the referral.

Frequently Asked Questions

Q: Is PHI stored in findhelp?

A: By default, demographic information is collected including name, phone number, email address, and zip code. Customers can choose to store additional information, including PHI, and are advised to follow their own policies for handling PHI.

Q: How is the data on your platform stored?

A: Data is stored encrypted with AES-256 bit encryption on the Google CloudSQL platform, a function-limited version of MySQL. Each customer's data is assigned a unique data label to allow logical separation of data and enforce access permissions. The Google data centers have undergone several security related certifications including ISO 27001 and SOC 2 Type 2 Certification.

Q: How is user data stored?

A: User information is stored encrypted and associated with a non-identifying token. Identifying user information is stored separately encrypted and only authorized authenticated users may join the user information with the identifying information.

Q: Do you have HIPAA policies and procedures?

A: **findhelp** is HITRUST certified, which incorporates HIPAA as well as NIST 800-53 security controls.

Q: Does findhelp conduct data privacy and security risk analysis or audits?

A: Yes, at least annually and upon significant system changes **findhelp** conducts risk analyses. We are HITRUST certified.

Q: Do you have a retention policy? If so, how long will you retain the records?

A: **findhelp** shall not keep personal information in a form that permits identification of data subjects for longer than is necessary for the purposes for which it was collected or to which the data subject has consented, except for legitimate purposes permitted by law, such as regulatory compliance.

Q: Do you have an incident response policy?

A: Yes, we have an Incident Response program as part of our broader Written Information Security Policy.

Q: Does findhelp use audit logging as part of its security program?

A: Yes; site actions as well as administrative site management tasks are logged to a central system that is monitored for security events.

Q: How else does findhelp ensure a secure platform?

A: **findhelp** conducts vulnerability scanning and penetration testing of the platform and follows secure coding best practices to keep the security of the platform up to date.

Q: How do your account policies help keep data safe?

A: **findhelp** requires all users to sign in with unique IDs to access any features other than the basic search functionality we make available to everyone. If someone fails to login correctly their account will be locked, and passwords expire and must meet minimum complexity requirements. **findhelp** follows the principle of least privilege to make sure users only have the minimum access they need for their role on the site.

Q: Does findhelp support role-based access?

A: Yes; **findhelp** supports defined roles as well as group membership to control access to information on the site.

Q: Does findhelp support Single Sign-On (SSO)?

A: Yes; **findhelp** supports SSO through SAML 2.0, allowing customers to leverage their own authentication methods including multi factor authentication.

Q: How can a user remove consent?

A: If a user no longer wants to share their information with a provider; the user can contact **findhelp** via **support@findhelp.com** and state that they are removing their consent. The **findhelp** team will remove the user's information from the provider's inbound referrals dashboard.

Q: How would user accounts be removed or destroyed?

A: If a user account needs to be permanently destroyed, **findhelp** does this by overwriting all PII for that user with non-identifying information, leaving only the non-identifying token as a placeholder.

Q: What is your Password Policy?

A: User Accounts:

Length: Minimum of 8 characters, Reuse: 3 (users cannot use any of the last 3 passwords he or she had used), Life: Maximum: 60 days, Complexity: Passwords have at least 1 lower alpha, 1 upper alpha, 1 number, and 1 special character.

Service Accounts:

Length: Minimum of 8 characters, Reuse: 10 (service accounts cannot use any of the last 10 password he or she have used), Life: Maximum: 365 days. Minimum: 1 day, Complexity: Passwords have at least 1 lower alpha, 1 upper alpha, 1 number, and 1 special character.

Q: Who is the data owner?

A: Customers own customer content, like assessment questions and staff generated notes. Seekers own their PII and referral information. CBOs own their screener and documentation. **findhelp** reserves the right to aggregate de-identified information to provide contracted services, like aggregate search activity in a region to help all customers with their focus and initiatives.

Q: Default user session timeouts and are they configurable?

A: We can set a timeout per white label, our default is 30 minutes and it can be changed to be 15 minutes

Q: Do we have a standard maintenance window?

A: Our standard maintenance window, when required, is Saturday 10:00 pm to Sunday 2:00 am Central time.

Q: In a closed loop system – what patient information is being sent to the referral partner / CBO?

A: Only the patient name and contact information is included in the body of the email. All other data is retained on the platform and requires the referral partner / CBO to log in to view additional information.

Q: How do you handle special privacy protections for populations such as alcohol and drug abuse patients, mental health or variations in individual state privacy protections?

A: We've developed multiple policies and procedures to ensure that the integrity of privacy is maintained for special populations and state-specific variations. We have solutions for role-based privacy, access to sensitive information is always limited to authorized and authenticated users, and our processes include user consent to determine access.

For additional questions, contact your CSM.