May 2020

Lighthouse Data Protection FAQ

Allies Against Slavery understands and values the concerns shared by many of our partners about client/patient data privacy and security. Ensuring you to feel confident entrusting your data with Lighthouse and Allies is a top priority, and we take your concerns very seriously.

As a web-based software application, Lighthouse is hosted on Amazon Web Services (AWS). Utilizing the AWS ecosystem, we benefit from Amazon's investments in advanced security practices, continuous monitoring and rapid response. The Lighthouse relational database was built to support organizations who must comply with HIPAA regulations, taking advantage of the best-in-class standards that have made AWS a platform of choice for several telemedicine and government applications. In addition to running in Virtual Private Cloud (VPC - our servers are isolated), an encryption layer has been added to all internal communication between our servers in line with industry best practices. Simply put, your Lighthouse data is stored privately, encrypted at the field level in transit and at rest, to provide the most secure solution to partners.

The following FAQs are intended to answer questions you may have.

What data is stored in Lighthouse?

Partners typically store the following information when using Lighthouse:

- **Organization Information:** This is basic information about the organization using Lighthouse, and can include name, address, programs, and program locations. This information is mandatory in order to use Lighthouse.

- **Person records:** This is basic information about an individual client screened and served by Lighthouse users. Person record information can include names, nicknames, initials, or case ID numbers from other case management systems. Some organizations store additional client-related data in a person record, such as birth dates, gender, and sexual identity. A unique person record ID is created in Lighthouse to correspond with each individual client.
    - *Note: Lighthouse users can add as much or as little client information or personally identifiable information in the system as they would like.*

- **Screening records:** This is a series of indicators, red flags, and questions observed during a screening of a client. A screening record also can include the program and geographic location of the screening, along with a screening conclusion regarding victimization. Multiple screening records can be documented and added to a person record.
    - *Note: Lighthouse users can add as much or as little screening information in the system as they would like. The more that is observed and included in screenings, the more effective Lighthouse becomes as you track trends and correlate red flags with victimization.*

- **Supplemental Information:** This refers to additional, optional data collected on clients/persons within Lighthouse. It can include CPS or law enforcement call IDs, education information, social media involvement, gang affiliation, tattoo photos, and other relevant information.

Will our data be safe, secure, and private?

Yes! We've taken the following steps with software architecture and protocols to ensure your data is stored safely and securely.

- **Database:** For data storage, we use a relational database service (RDS) hosted by Amazon Web Services (AWS). Amazon RDS makes it easy to control network access to your database. The Lighthouse database was built using an architecture that enables organizations to comply with HIPAA standards.

- **File Storage & Encryption:** The underlying database files storing the data are encrypted using AES-256 server-side encryption. The data is encrypted end to end, in transit and at rest. Communication back and forth between the user/application, the server, and the database is encrypted the entire time using SSL.

- **Privacy:** The database runs in Amazon Virtual Private Cloud (Amazon VPC), which enables us to isolate the databases and securely connect to your existing IT infrastructure. Your data is private. No other Lighthouse partners can see or access your data, unless you have an established MOU or other data sharing agreement granting them access. Data access is restricted to a limited number of trained Allies' employees. Our data environment also restricts the data elements accessible to employees, such as Personally identifiable information (PII), to a need-to-know basis. The only individuals with database access, outside of the Allies team, will be data engineers who solely manage the infrastructure. They are not, as a practice, accessing individual level data and PII, and they are subject to privacy and nondisclosure agreements.

How will the data be used?

The primary use of Lighthouse data is to empower partners/users to identify suspected and confirmed victims of sex trafficking and exploitation. We want you to see, understand, and use your data to respond effectively. The secondary use of the data is to improve de-identified, aggregate trends and insights for the collaborative groups, such as Coalitions, and research efforts. Uses may include:

- To allocate and direct resources to victims and potential victims of human trafficking;
- To provide information to governmental, educational and charitable groups studying or trying to prevent or otherwise reduce human trafficking;
- To identify and publish patterns and trends in human trafficking; and
- To further refine the usefulness of Lighthouse and operations thereof as well as other programs to counter/raise awareness of human tracking.

As a rule, these additional uses of data do not include PII and pertain solely to de-identified, aggregate analysis. Allies and Lighthouse partners enter into a software use agreement further outline protections for and uses of the data, and partnerships are also covered by a privacy and non-disclosure policy.

Additional Questions?

Contact John Nehme, Allies President & CEO, at john@alliesagainstslavery.org.

Date: May 2020