Long Beach Continuum of Care contracts with Bitfocus, Inc. (Bitfocus) to maintain and host HMIS services using Clarity Human Services HMIS (Clarity). Purpose-built for use as a Homeless Management Information System (HMIS), Bitfocus designed Clarity from the ground up to meet or exceed the requirements put forth by HUD and the federal partners, including data privacy and security requirements. The system fully complies with the criteria established in the HMIS Proposed Rule and 2004 Data and Technical Standards Notice. Bitfocus turns to HIPAA as a guide when expanding upon the current HUD privacy and security standards. Clarity is a fully HIPAA-compliant case management solution.

Clarity's security features and controls:

- **Multi-factor authentication:** System administrators can supplement standard user credential with a rolling-code based Two Factor Authentication (2FA) requirement for added security. And, where necessary, System Admin can limit access at the device level. 2FA is a form of multi-factor authentication that requires two separate pieces of information to confirm the identity of a user attempting to log in to the system. When 2FA is enabled, users must enter both a password and a 6-digit verification code to log in to Clarity Human Services. They can receive the verification code through their email account or through an Authenticator App.

- **Password policy enforcement**: Clarity has several levels of login security to ensure client information is secure. Clarity automatically enforces policies around password complexity, maximum login attempts, self-service recovery, and other password settings. Password rules requires users to meet a minimum level of complexity. System administrators can force a password reset after a specified number of days. Users can reset their own passwords within Clarity or with the "FORGOT PASSWORD?" function on the login page which references users' email address saved in their Clarity user profiles. Accounts are locked after 3 failed attempts and only the System Administrator can unlock accounts.

- **Encryption**: By default, all Clarity Human Services traffic is 2,048 bit SSL encrypted at transit and at rest. All API traffic must be further AES encrypted. Each instance of Clarity operates under a separate hostname with a dedicated MariaDB database dedicated to it. Other customer data is never intermixed. Employees with access to customer data are required to sign confidentiality agreements, and their use of the system is logged for auditing purposes.

- **Detailed Audit Logs**. Clarity Human Services stores every change to a client record and offers authorized users with a full audit trail of every data field in the system. Audit trails are assessable by two methods: Audit Logs and the Database. Audit Logs display any updates made to any of the data on the associated forms. Items such as the previous value and updated value of a field, the date/time of the update, and the end user who made the update are all historically presented in a concise format. The Database allows the System Administrator to access the data using a query tool or write reports to manage the updates in any way the System Administrator defines.

- **Flexible sharing and access controls**. A combination of system-, project-, user-, and field-level controls empower system administrators to tailor access to the minimum amount necessary to get the job done.

- **Physical Controls**. Bitfocus' data center employs established best practices for physical access control, including round-the-clock security and technical staff, dual-factor authentication access, biometric scanners, and monitored security cameras. Off-site backup and supplemental storage are hosted in the AWS Cloud.

  Bitfocus maintains its own physical server infrastructure, hosted at a HITRUST CSF compliant data center that undergoes annual independent audits. Bitfocus code base undergoes on-going security reviews, including third-party penetration and vulnerability testing.

- **Unauthorized Access**
  In the event of unauthorized access to the HMIS and/or client data, or if there were suspicion of probable access, Bitfocus will take the necessary steps to mediate the situation. The system will be examined to determine the presence of system or data corruption. If the system has been compromised, Clarity would be taken offline. Bitfocus loads the backup copy of the system data onto another server. Bitfocus investigates the extent of the unauthorized activity/corruption and corrective action needed. The finding would be reported and options to remedy the situation would be discussed with the HMIS Administrator.

Long Beach HMIS System Access

Agency Participation
Prior to participating in HMIS agencies are required to sign an Agency Agreement (3.1.1 – CoC-Funded Projects, 3.1.2 – Non CoC-Funded Projects).

User Participation Agreements and Training
Program providers and users are required to attend training and sign user agreements prior to accessing the HMIS (3.1.3.1 – New User, 3.6 – Training). The training includes information on "Ethics, Security, Privacy Practices and Client Confidentiality" (3.6 – Training).

Level of Access
The system is setup with multiple user access levels to limit who can view and/or modify the client's data. Each user access levels allow different access rights and abilities to various sections of the systems.

Physical Access
Access to HMIS, through the use of laptops or other devices, must adhere to HMIS Policies and Regulations (User Agreement, Agency Participation Agreement). Program participant information should never be left unattended (User Agreement). To decreases potential viewing and/or manipulation of client data by unauthorized individuals the system automatically logout users who's been idle for 30 minutes. However, users must logoff before leaving work area (User Agreement).

Hard copies of program participant information must be kept in a secure file (User Agreement). When hard copies are no longer needed they must be properly destroyed to maintain confidentiality (User Agreement).

User IDs and Passwords
Users are issued a unique User ID and password for entrance into the application. Users are prohibited from sharing the assigned User ID's and Passwords to access the HMIS with any other organization, governmental entity, business, or individual. (3.4 – Participation Integrity; User Agreement). User IDs and Passwords must be kept secure (User Agreement).

The passwords must be 8 to 16 characters in length and must contain at least one uppercase character, one lowercase character, one number and one non-alphanumeric character. If user login failed four consecutive attempts the users need to contact the HMIS Administrators to reset the password or reset by clicking on "FORGOT PASSWORD?" on the login page. The security feature prevents access to the site by a password generator. Passwords automatically expire every 45 days requiring the user to create a new password. The new password created cannot be used previously. Users are allowed to login into one terminal at a time.

Minimum System Requirements
Workstations accessing the HMIS are required to have "Antivirus and Anti-Spyware with most recent data protection download" and "Firewall Security" (3.5 – Minimum System Requirements). For all Agencies are required to keep updated virus protection, anti-spyware and firewall software on Agency computers that access the HMIS and will follow the recommendations outlined in the HMIS Access Requirements document (Agency Participation Agreement IV.8.).

Security Breaches
The HMIS Administrator must be notified immediately of any noticed or suspected security breaches (User Agreement).

Unauthorized Access
Any unauthorized access or unauthorized modification to HMIS information or interference with normal system operations will result in immediate suspension of user access to the HMIS (User Agreement).