Birthrate Plus® Acuity App information for Trusts

S E C U R I T Y

Servers

The app runs on 2 virtualised Linux based server platforms running Ubuntu Server 16.04 LTS on the 4.4.* kernel (at time of writing).

The servers are privately networked. The database server is not publicly accessible and is firewalled to only allow connections from the application server.

Application server
NGINX 1.14.0
PHP 7.2

Database Server
MariaDB 10.0.38

The servers are patched weekly with immediate patches for critical updates as they are released.

The server and app currently have no failover or load balancers. So, if the servers were to crash there is no redundancy in place. The servers would need to be restarted manually by the Laser Red technical team.

Datacenter

Security controls provided by our datacenter facilities includes but is not limited to:

- 24/7 Physical security guard services
- Physical entry restrictions to the property and the facility
- Physical entry restrictions to our co-located datacenter within the facility
- Full CCTV coverage externally and internally for the facility
- Biometric readers with two-factor authentication
- Facilities are unmarked as to not draw attention from the outside
- Battery and generator backup
- Generator fuel carrier redundancy
- Secure loading zones for delivery of equipment

Only select engineering teams have direct access to the backend servers based on their role.

The data centers are supported 24/7/365 so any server or network issues are constantly supported, however they do and will not support the app on the server in any way. Support for the app can only be provided by Laser Red.

SSL Certificate

The application is now using SSL for all connections, meaning all data transfer is encrypted to and from the app.

Backups

Backups of the data occur daily at 4am, this is a full atomic dump of the current database. Snapshot backups of the servers take place weekly.

Data

Data is stored centrally, but is only accessible by each trust, and the Birthrate Plus® administration team. No Patient Identifiable data is entered in system. it is purely numeric. Data is as secure as is reasonably possible.

The application does not keep audit logs of user activities. Server access logs are available to Laser Red. Additionally, the datacenter hard drives and infrastructure are securely erased before being decommissioned or reused.

Passwords

The system uses an 8-character password policy. All passwords are strongly bcrypt hashed and salted. All servers are patched regularly, require an authorised public key for shell access and are firewalled

Support Availability

Currently the acuity app only has technical support in normal operating hours - 9am till 5pm Monday to Friday, excluding public holidays.

The Birthrate Plus® Acuity App was designed and developed by Laser Red, a digital agency based in Lincolnshire. Any support or technical information should be directed to the Birthrate Plus® Team who will then liaise with Laser Red.

Support is only available to the Birthrate Plus® Team, not end users.