Datacon Security

System
Your Datacon server software operates on an Apple Macintosh running macOS.
macOS (previously Mac OS X and OS X) rarely suffers malware or virus attacks and has been considered less vulnerable than Windows. We recommend using a Mac without a screen. This reduces the possibility of a user accidentally downloading malware through emails or web browsing which could compromise the server.

Software
Our server software creates a virtual computer - a computer within a computer. This virtual computer implements a non-standard chip and operating system that hosts the Datacon software. This virtual operating system has it's own file system and does not have direct access to the macOS command shell or file system. There are no publicly available compilers or tools which allow software to be created that can run within our virtual system.

Data
The Datacon Dental System implements a proprietary database that is not usable without our software. Unlike many other systems, access to raw data is not possible using a standard database such as SQL, Access or Filemaker. There are no APIs that allow outside software access to our data. Protected patient data items such as name, birthdate, social security number, and treatment history are stored in separate files. Without the benefit of the software, the data in one area cannot be tied to the data in another area. For instance, a patient name cannot be connected to a social security number. We do not store credit card numbers when patient payments are processed. All access to our database must be done through the software and is password protected. Each user has their own password and there are privileges associated with each user that can limit access to different areas. All access to the system is logged.

The storage on your Macintosh server is divided into two partitions, one for the operating system and our software and the other for your data. The data partition can be encrypted and the privilege to 'open' the drive after a power failure can be granted to specific users.
When a backup is performed, the data partition is copied to an external drive . We do not back up the server software with the data. A person with a backup cannot access the database without procuring, installing and licensing a copy of our software. We recommend the use of encrypted backup drives to protect documents stored in patient folders and to prevent access to archived reports.

Remote Access
Individual users can be granted the privilege of accessing the software using our client software from home or remote locations. This communication is password protected and encrypted. In addition, it is possible to whitelist a set of specific IP addresses that may access the data.

Our Datacon Mobile option provides a secure means for a doctor or staff member to access specific information using a web browser on a remote workstation, laptop, tablet or phone. Our server software implements this using a custom secure web server using HTTPS over TLS connections. Our web server does not allow direct access to the file system. All responses are handled by software code which can limit access based on user privileges and job description.

Our DDS Zone option adds an additional layer of security by routing all access to Datacon Mobile through Cloudflare. Cloudflare, Inc. is an American web infrastructure and website security company, providing content delivery network services, DDoS mitigation, Internet security, and distributed domain name server services. When DDS Zone is configured, your server only responds to connections from the Cloudflare servers.

Our Secure Email option provides a means for the doctor or staff to send emails containing protected information through a HIPAA compliant service.