

## ***Business FTP Service & HIPAA Compliance***

Maytech provide hosted FTP service to business and public service worldwide. We have many customers in the healthcare industries and recognize the importance of confidentiality and security when handling protected data. As Maytech merely provides an electronic delivery service as opposed to a data processing service we are not a HIPAA Covered Entity nor a Business Associate for HIPAA purposes

Our service is designed to offer strong security and data integrity with many features (both standard and optional) that we believe allow you to meet the HIPAA technical standard in the use of our service.

The following procedures may be relevant:

- Rigid control of access to your Maytech control panel login and to FTP logins by the use of difficult to guess passwords which should include a combination of upper and lower case letters, numbers and other characters;
- Issuing passwords only to trusted personnel and changing passwords regularly;
- Using only our FTPS encrypted transfer service for file uploads and downloads;
- XCRC data integrity check.
- End-to-end data encryption.

The above are only recommendations and you should take independent advice to ensure that your contemplated use of our services, as any aspect of your data handling, is HIPAA compliant.

The information below may assist you in making further determinations with regard to use of the Maytech FTP service and HIPAA compliance.

### **Physical Security**

Maytech servers are located in private suite at Redbus Interhouse, London E14 and NAC Cedar Knolls NJ, USA. The buildings benefit from strong physical and electronic security, uninterruptible power and fire suppressant systems.

### **Firewall**

The Maytech networks are protected by a stateful packet inspection firewalls.

### **Operating Systems**

The FTP service is based on Dell 1850 servers running Redhat Enterprise Linux. Servers are automatically updated from Redhat with all available security updates.

All ports, other than those required for the provision of service are closed.

### **Customer Access**

Customer access to the FTP servers is restricted to the FTP protocol, we do not offer access via other protocols such as SSH or telnet. All sessions are automatically terminated after five minutes inactivity.

## **Encryption**

Customers login to the control panel over HTTPS, this traffic is therefore always encrypted.

Maytech offer FTPS (FTP over SSL) as an optional extra where encrypted file transfer is required.

Further data security and integrity technologies are available to you. Consider end-to-end encryption using PGP or other strong encryption technology. Some FTP software including CuteFTP Professional has built-in support for public key encryption.

## **Data Integrity**

Our servers are XCRC enabled. This is a protocol supported by some FTP client software, it provides a cyclic redundancy check to ensure that data has not been corrupted in transfer.

## **Confidentiality**

Customer data is held in discrete file areas and can never be visible to other customers. Additionally data for each FTP login is invisible to other logins.

## **Data Persistence and Backups**

Although Maytech provide a high-availability service using RAID arrays and failover server clusters, we do not keep permanent or incremental backups of customer FTP data. File deletes are permanent there are no persistent copies of the data.

Revised 28<sup>th</sup> June 2007  
<http://www.maytech.net/>