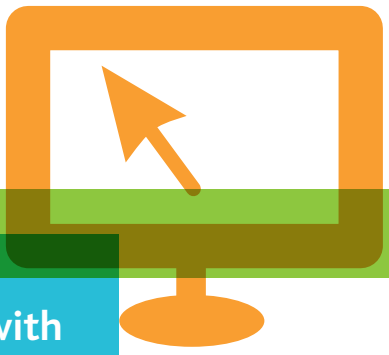
CAPITA

Mobile Device Management Service



The freedom of anytime, anywhere access with the assurance that clinical systems and patient data are secure.

There is a growing demand among healthcare professionals to enable mobile devices such as smart phones and tablets to be used in supporting patient care. The use of mobile devices can enhance the quality of care by bringing patient records and information to the point of care. This coupled with the increase in clinicians working across multiple sites and the limited number of available PCs is to users is putting pressure on NHS Trusts to allow either organisation supplied or staff owned mobile devices.

Adopting mobile devices brings challenges including:

- Ensuring patient data is secure and information governance policies are adhered to
- Maintaining system performance for the end user
- Management of the devices, particularly with staff-owned devices which use a variety of operating systems, numerous applications and hold personal data

Mobile Device Management Services

Capita's Mobile Device Management (MDM) service can be adopted to support health organisation's develop a mobile device policy as well as deploying an MDM solution which can support both organisation supplied and staff owned 'Bring Your Own' devices.

It provides the ability to:

- Configure and update device settings
- Enforce security policies and compliance
- Secure mobile access to clinical systems
- Monitor usage and manage performance
- Deploy as a on- premise or cloud hosted service

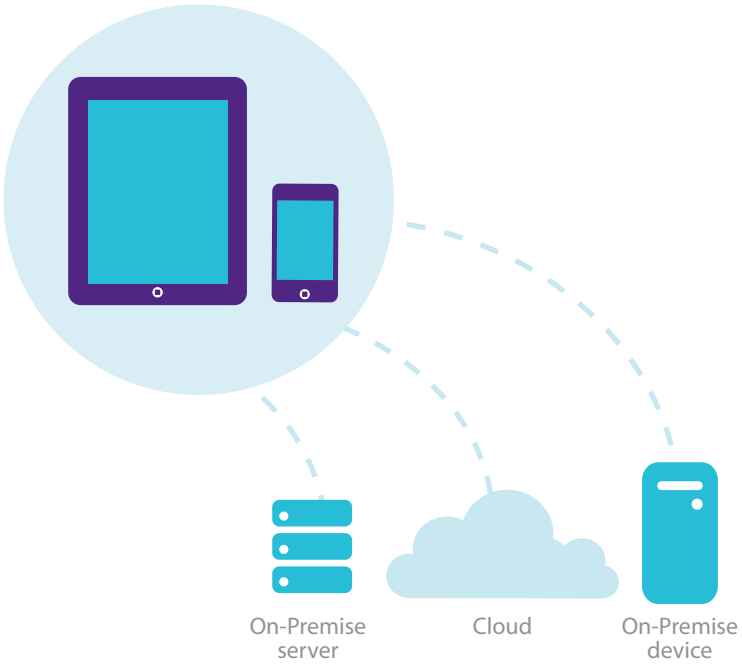
Key features of the solution include:

Configuring

IT departments can set device and user profiles for access, based on each organisation's own policies. They can also distribute and manage all purchased applications and provide secure mobile access to documents and systems.

Deploying

Deploying the MDM service on devices is simple and doesn't rely on resources from the IT department to complete. Activating the device to receive services such as email can be completed remotely by the device users.



MDM Deployment Otions

Published: 27/03/13

Securing

Policies can be applied to devices and software on a per user basis. These policies can be mandatory and can be set dependant on the device type and user. For example the camera can be disabled on the mobile phone or tablet. Security features include:

- Passcode enforcement
- Selective data wipe
- Jailbreak/root detection
- Data encryption
- VPN configuration
- Data leak prevention
- Email settings configuration
- Wi-Fi network settings configuration

Monitoring

Remotely change settings on the device, for example, if a new wireless network is installed, or VPN settings changed, configuration profiles can push these new settings to the devices. Any settings that can be set manually on the device can be managed remotely.

Managing

Remotely change settings on the device, for example, if a new wireless network is installed, or VPN settings changed, configuration profiles can push these new settings to the devices. Any settings that can be set manually on the device can be managed remotely.

Supporting

The MDM service tools provide the IT department with remote support capabilities for devices, including passcode reset, remote locking if the device has been misplaced, remote wipe to factory settings if permanently lost and diagnostics to identify any issues.

End users can also access self-service support via a web browser. If for example their device has been lost, they can log in and remotely wipe to factory settings.

Supported Devices

Capita's recommended MDM service tools support:

- Apple iOS (iPhone, iPad, iPod touch)
- Devices from the major Android phones and tablets such as Samsung, HTC and Motorola
- Microsoft Windows Phone 7.5
- Blackberry
- Windows Mobile
- Some older legacy OS devices

Benefits of Capita's Mobile Device Management Service:

- Supports improved delivery of patient care as clinicians can access patient data at the point of care
- Improves working efficiencies and supports the increase in clinicians who are based across multiple sites
- Ensures you have the knowledge to enforce security and compliance in terms of access and usage
- Simplifies IT management with centralised configuration and monitoring including fast provisioning of new devices and consistent security policies
- Can reduce the need to invest in devices with the option to offer a 'Bring Your Own' device policy

Capita Managed IT Solutions Hillview House, 61 Church Road, Newtownabbey, BT36 7LQ Tel: 0289085 9085 mits@capita.co.uk www.capita-mits.co.uk