Bring Your Own Devices (BYOD) Information Governance Guidance

1. Purpose

The purpose of this document is to provide guidelines that will support organisations considering whether to enable the use of Bring Your Own Device (BYOD) within a care environment and minimise the risks (which can be significant) associated with their use. The IGA recommends a default policy position which prohibits the use of personal devices where an organisation lacks the technical expertise and resources to implement BYOD safely. Local policies on BYOD need to be enterprise wide and approved by the executive or senior management team.

This short guidance does not identify specific technical controls or solutions, nor does it endorse particular vendors or products. Reference to any specific product, process or service by trade name, trademark manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by the IGA. Those intending to support BYOD arrangements should also refer to BYOD guidance provided by CESG[1] on behalf of the UK government and to guidance provided by the Information Commissioner[2].

2. Developing the case for BYOD

In anything but the smallest organisations the implementation of BYOD represents a major decision that should be supported by a formal strategic and full business case considering the following:

- Is there a strategic case e.g. taking account of the NHS 5 year plan, the organisation's strategy, IM&T strategy?
- Technical case - e.g. what is the capacity of existing Wi-Fi?
- Financial case - does it save or cost money?
- Consultation – e.g. would staff want to bring their own devices? Do they understand the risks and responsibilities?
- What are the privacy risks? A Privacy Impact Assessment (PIA) is recommended.

3. BYOD Policy

All organisations must develop their own BYOD policy (as a component of their broader security policy), following a thorough risk assessment. Where personal data may be held on devices a Privacy Impact Assessment (PIA) should be undertaken[3]. A correctly completed risk assessment enables an organisation to demonstrate that a methodical process has been undertaken which can adequately describe the rationale behind any decisions made. This must identify and resolve issues such as:

i. Which devices and operating systems are, and are not, acceptable to the organisation? It may be that an organisation only supports devices from a specific manufacturer, or which can be successfully managed by Mobile Device Management (MDM) software.

[1] The Communications Electronics Security Group (CESG) is the UK Government's National Technical Authority for Information Assurance https://www.gov.uk/government/collections/bring-your-own-device-guidance
[2] Information Commissioner: Bring your own device (BYOD) https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf
[3] https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

ii. What are the potential impacts on live services?
iii. Whether the organisation could provide more choice to users in what corporate devices are issued, thus removing the need for BYOD (so called 'Choose Your Own Device' or CYOD).
iv. Who is responsible for ensuring compliance with licensing requirements? Organisations are ultimately responsible for ensuring sufficient licences are in place for all devices which connect to corporate systems. Whether those licences are funded by the organisation or the individual must be clarified.
v. How to ensure security management and application control software acceptable to the organisation (e.g. industry standard) is installed.
vi. Managing staff role/function changes, in particular when staff leave the organisation, which may require data removal and/or different access privileges.
vii. Security incident management plans – it must be ensured that users can report the loss of devices and consequently that security actions can be taken. Once the incident has been logged there must exist incident management procedures for the appropriate security steps in line with local policy.
viii. Whether there will be any re-imbursement of charges or a contribution towards the running costs of any device used extensively for business purposes.
ix. Use of a remote wipe function in the event of loss or theft and whether this would wipe the owner's data as well as work-related data.
x. Will work-related data be segregated from the owner's private data? Are there classes of data that are not suitable for BYOD?
xi. What are the training requirements for staff?

4. Acceptable Use

The BYOD policy must be linked with an Acceptable Use Policy (AUP), either as a corporate policy or something each individual signs up to, which must cover:

i. Whether there are requirements (strongly recommended) for the personally owned device to be inspected by the appropriate IT security staff (potential access to private information).
ii. Whether use of the device may be restricted outside of the controlled corporate environment.
iii. The requirement for a mandated minimum security requirement (e.g. encrypted hard drive, up-to-date AV, strong passcodes).
iv. The requirement for the AUP to cover how corporate information and services can be used and what is acceptable behaviour during working hours.
v. Recommendations for safety and security when working outside a secure office (e.g. eliminating "shoulder surfing" and possible theft of equipment).
vi. Business continuity requirements. What are the user responsibilities if BYOD kit is unavailable/inoperative? Does the user have to take personal time to replace it during working hours? How quickly must the user replace it?
vii. The minimum equipment specs needed to take into account user health and safety and accessibility.
viii. Whether the whole device or just the corporate data will be remote wiped if the device is compromised?

5. Understand the legal and issues and licensing requirements

Both the organisation and its employees need to be clear about legal responsibilities and how they will be met where BYOD arrangements are in place. These include:

i. The organisation needs to decide whether the device can be shared for use with family and friends and, for example, the organisations liability in cases where information belonging to individuals who are not employees (who are not subject to the AUP) may be accessed, viewed, wiped or otherwise processed by the organisation as part of the organisation's commissioning and ongoing management of the device.

ii. Organisations must ensure that they are fully aware of the implications of confidentiality, Data Protection Act (DPA) and Freedom of Information Act (FOIA) and the complications arising from data being stored in multiple locations and potentially overseas (which may well be unlawful) if employees take devices abroad. Data held on an employee's own device is still the responsibility of the employing organisation and may need to be located and shared quickly in order to meet legal requirements.

iii. Employees should understand BYOD devices will be subject to the same policies and legislation (DP & FOIA) as corporate devices (this may be limited in cases where business and personal use is segmented.

iv. Health and safety requirements must be understood and addressed so that staff claims of detriment or being required to work in unsuitable conditions are prevented.

v. Licensing models for operating systems and applications are complex and diverse. The organisation must ensure it thoroughly understands the licence requirements appropriate to the BYOD solution being developed. NHS organisations that retained the Microsoft Volume License Services (MVLS) on the same volume and versions, should ensure adequate license coverage, especially if making available a local mail service on BYOD.

6. Two Factor Authentication

Access to organisational networks (and NHS networks) should be secured via two factor authentication ("something you have" and "something you know" are the most common).

Examples of "something you have" may be:

- A cryptographic certificate on a device which is securely managed by an MDM system
- An NHS smartcard,
- An RSA secure authentication token,
- A biometric such as a fingerprint.

Two factor authentication can be seamless (e.g. using a certificate) or challenge response (token).

7. Secure handling of sensitive/patient or service user data

Mobile devices are inherently less physically secure than traditional IT equipment physically connected to the organisations network on its own premises. Consequently all sensitive and confidential data must (at the very least) be protected through appropriate device level encryption.

A range of potential mechanisms exist to ensure data are protected at all times and local risk assessment must be used to identify the appropriate solution and how it can be securely integrated into existing secure networks.

i. Individual sandbox applications
These are applications which manage the data they hold in a secure encrypted manner which prevent it being accessed by other applications. An example of this type of application would be calendar/email on the iPhone, controlled by Exchange Mobile Device Management (MDM). This ensures that calendar / email residing on the mobile device is adequately protected through access controls, all data is held in an encrypted manner and the information can be remotely wiped if the device is lost or the user leaves the organisation.

ii. Sandbox environments
A controlled environment in which multiple applications can exist and local data can be stored. This controlled environment is managed by the organisation, all data that resides within it is encrypted and again the information can be remotely wiped if that becomes necessary.

iii. Remote environments
In this example the mobile device hosts a remote connection or virtual desktop which enables access to applications and data on the secure network. Sensitive data is never stored on the mobile device and consequently the risks of loss or exposure are reduced.

iv. Non-protected applications and environments
If the organisation does not have the capability (or it is unfeasible) to sandbox the application/environment or utilise a remote environment, but still requires sensitive data storage, then the employee's device should be secured in an identical manner to the corporate device with same AUP in place (including wiping the device when access is no longer required). Organisations should be aware that essentially this means that employees are loaning their device to the organisation.

8. Circumvention of built in Operational Security (OS) controls

The bypassing of manufacturer and security controls that are implemented by default is referred to as 'Jail breaking' or 'rooting' and is a common activity. There are numerous tools freely available to allow devices to be unlocked and arbitrary software installed or stored data accessed. Where possible installed applications must be capable of operating in their own secure space on the device (sandboxing – see above) to ensure that any data remains encrypted in the event of the device being jail broken or otherwise compromised. Any device which is identified as having been jail broken or rooted must be prevented from accessing any personal or sensitive data.

9. Cloud services

Many mobile devices offer the ability to automatically back up their contents to Cloud services. Cloud services being enabled by default can result in sensitive data being uploaded to remote servers without the user being aware it has happened or sanctioning it. These servers may be anywhere in the world and may be out of the jurisdiction of the organisation responsible for that data e.g. the country in which the cloud server reside may not have the same level of data protection laws.

Unnecessary services should be removed or disabled prior to use and the ability to re-enable or reinstall them restricted or blocked completely. The ability to transfer data from the device to other networks or devices should be restricted to a 'whitelist' of permitted destinations where it is possible to do so.

Ideally the sensitive data should reside in the protected environment/application which is unavailable to the cloud service whilst the personal information can be backed up to a cloud service (if required).

Alternatively, organisations should be aware that while many of these devices rely on access to their related Cloud services to perform backups, an alternative means of backing up data on the devices may need to be identified. If organisations choose to back up devices locally they should be aware of the storage impact and legal implications of potentially retaining employee personal information. Employees should understand and consent to the impact on them through the AUP.

10. Consistent policy/control

Where there is a mix of personal and corporate devices in use then lack of consistent policy or control over mobile devices can result in sensitive data being copied to insecure devices or locations unless users accept the same levels of control over personal devices as are in place for corporate issue items.

Where an organisation allows the use of personal devices for business purposes this should be supported by documented agreements with staff and technical security controls to protect information with the aim of ensuring critical and sensitive information handled on personal devices receives the same level of protection as that provided by corporate-owned equipment.

11. Control/monitoring of devices

All devices on which personal data or other sensitive information may be stored (or from which sensitive information may be accessed) must be under appropriate control of the organisation. Organisations should consider the implementation of Mobile Device Management (MDM) solutions to provide central management of policy, device profiles, configuration and access controls. It should be noted that having an MDM in situ does not necessarily represent a complete BYOD management solution.

Organisations should treat BYOD devices as personal devices and not corporate devices with regard to connection to corporate WIFI where this enables access to corporate resources. It should be noted that it is possible to have secured the information on a device through sandboxing but the device itself may have become compromised (e.g. through malware) without the organisation or the user being aware.

Policies regarding the wiping of sensitive configuration/data from devices should not be totally framed around the normal leaving procedures. They should include mechanisms to be enforced in the event that a member of staff leaves as a result of disciplinary processes.

The organisation must ensure that the user consents to the requirements of the organisation to monitor the use of the device e.g. the potential requirement to be able to geo-locate devices or the need to monitor internet traffic.

Organisation should retain the right to audit devices to observe whether the technical and procedural controls are effective. It would be good practise to dip sample a random set of devices on a regular basis.

12. Bad Practice BYOD Implementations

The most important feature of any BYOD implementation is that it should be effectively managed and all the risks and appropriate controls considered. Organisations can sometimes find themselves implementing BYOD by the back door and thus expose themselves to unrecognised risks. It is essential that organisations are alert to, and prevent, BYOD implementations which include:

- Personal devices with access to corporate resources with no controls e.g. adding a corporate local mail service to unmanaged personal devices.
- Making sensitive corporate systems too widely available to any device with insufficient registration confirmation of whether it is a trusted device.
- Making BYOD available without any controls to a small number of staff (such as the executive management or IT Department) reasoning small volumes is an effective control. This can be compounded by the trickle-down effect to other staff groups or where there is not a rigorous registration process details or how to “get works mail on my own phone” can leak out.
- Not having a register of BYOD devices and their owners and not ensuring data removal when employees leave an organisation.
- Implementations where there is a mix of corporate and personal data on devices to the extent they cannot be unpicked.

13. Benefits Realisation

Any benefits realisation (including potential cost savings) should take into account the organisational cost of ownership of BYOD devices (employee reimbursement, licensing, infrastructure and support) and the results of local risk assessments. BYOD may have hidden costs – whilst an organisation may see benefits in the lack of capital spend on IT equipment, and a “happier” workforce using their own equipment, the number of mobile OS and versions make supporting the equipment potentially costly. Older versions of both OS and apps tend to have been patched for operational and security reasons – so there is a potential for reduced security on older devices, apps and OS. The organisation may also incur costs downstream if health and safety requirements are not effectively addressed.