Implementation Guide for Healthcare

Author: Rob Blagden
Version: 1.1
Date Created: 08/03/2020

Engage your people all the way through

#PeopleBeforeTechnology
Introduction

BYOD is used across the globe to offer flexible working arrangements for employees and there is evidence which shows it can improve innovation, efficiency and morale. There is a strong desire in the workforce to have choice in whether they use their own device for work tasks. Organisations can potentially benefit from a more engaged and productive workforce whilst helping to manage down technology costs. There are sustainability advantages from using BYOD reducing the environmental impact of raw material and power consumption.

In a 2019 Twitter survey there was an overwhelming desire from employees for BYOD.

Over 80% of respondents said they wanted to use their own device for at least some work tasks.

In another survey 92% of organisations, not offering BYOD, said it was likely or very likely that staff were already using personal devices in the workplace regardless of policy.

81% of the organisations surveyed thought BYOD was definitely or probably beneficial.

BYOD offers a wide range benefits for both the employee and the organisation.

But...the NHS has a range of unique challenges that require special focus above and beyond the needs of other organisations.

For instance:

- Does the value of patient data alter how BYOD is secured in the NHS?
- How will clinicians maintain a healthy work/life balance if their personal smartphone also provides intrusive alerts on the condition of their patients when off-duty?
- Is there benefit from BYOD if the most useful data lives in legacy systems which limit accessibility and flexibility?
- How can a standard approach be used when the knowledge and risk appetite in each NHS organisation is far from standard?
- In large NHS organisations with a range of roles and systems how do you ensure solutions maintain digital equity and avoid digital division?
A key discovery in a recent study revealed 37% of organisations offering BYOD don’t have policies. In the NHS this rose to 44%. Often where policies are provided, they are confusing and difficult for employees to access. Where policies do exist only 36% of those surveyed said they had an audit or monitoring process.

Organisations did believe there were benefits in offering BYOD and the survey data revealed a likely uptake in a number of key areas shown below. Blue areas are usage reported today and the red areas indicate uptake if BYOD were available.

There is no single implementation methodology for BYOD in the NHS because every organisation is different. Size, culture, ambition and leadership will all influence your specific implementation journey. Keeping BYOD optional is important but so too is maintaining equity and avoiding a digital divide.

This guide is the result of a yearlong study into BYOD in the NHS. It is not a set of instructions on how to safely and successfully roll out BYOD, rather it presents a list of suggestions and questions you might want to consider to help your project.

It is hoped the information provided will inform the BYOD approach that is right for your organisation.
1. Engage colleagues all the way through

In every project, but especially technology projects, people are the most critical aspect. The human interface between electronic systems and real-world processes is often where unexpected outcomes can occur and maintaining an open dialog is essential to success. The engagement suggestions below are not exhaustive so find the methods that work for you. Many projects have failed due to a lack of engagement, use techniques at the start of your project but also at every stage of your project to ensure people are connected with what you are doing.

- Use workshops throughout to gather views and be willing to accept there will be differences of opinion.
- Work closely with staff to review how BYOD could be beneficial for the colleagues, the organisation and service users.
- Consult staff on ways they already benefit from using their own device.
- Have impartial experts available to provide guidance and advice to support the conversation.
- Listen to staff perspectives on the safety of patient data and the concerns about the potential impact to work/life balance.
- Clinicians need assurance the organisation won’t proceed to offer clinical system access via BYOD on day one without adequate controls, their input and confidence needs to be highly valued.
- Gather a list of the areas where there is agreement BYOD could add value.
- Dig deeper into the areas of consensus and discuss the impact and risks openly and honestly.
- Form a group to take the project forward and include clinicians, IG leads, those with the biggest concerns, board members and those keen early adopters.
- Board leadership and support is key in a digital change project.
2. Develop your scope

There are a range of levels to which you can implement BYOD, it doesn’t have to be an all or nothing approach. Scaling up over time by starting with low risk but high benefit apps will build trust in BYOD. Building confidence in systems is just as important for technical teams as it is for others.

- Agree on the initial objectives and outcomes.
- What are the specific use cases? Initially perhaps these will be business applications with wide appeal rather than clinical. Also consider applications which will make a difference to clinicians; perhaps rotas, secure messaging apps or reference data to support clinical practice.
- Who will your users be and are they interested in BYOD solutions?
- If you don’t offer email or calendar these could be good starter BYOD applications because they have wide appeal. Having access to a calendar on the move can be really useful and doesn’t require users to have the latest or best smartphone device.
- Talk with other similar organisations who already use BYOD about where they have seen the maximum benefit.
- Are there areas of weakness that BYOD could help you address? For instance, there is evidence BYOD can increase employee satisfaction, productivity and innovation. There are studies which have proven a link between employee retention and BYOD. Could BYOD be a differentiator for your organisation in some form?
- Once decided think about total number of users that could utilize the solution and who might form a subset to engage in a pilot to test solutions and assumptions.
3. Deep dive governance

Setting up appropriate governance for your BYOD implementation is essential. In research it was found that clinical staff had significant concerns about BYOD in terms of data security and being free from intrusive alerts when not at work. Reviewing processes will help address these concerns.

In a survey question asking for people’s reaction to BYOD the feedback was generally positive, although the focus organisation’s response was mixed because of clinician concerns over data security and expectations the organisation may place on them.

Here are some steps to help you think about system and data governance:

- Review the planned scope and break down in detail exactly what data will be required, where it exists today and how it will be managed.
- Limit data to what is required to enable the anticipated outcome.
- Classify the types of information and have clarity on whether any is confidential or personal identifiable data (PID) and who currently owns it.
- Think about how data will be transferred, accessed and stored on devices.
- Prioritise presenting/streaming data to BYOD rather than storing data on devices.
- Be clear where the data ownership responsibility applies regardless of processing device.
- Think about how you will protect staff from alerts when they are not at work.
- Start documenting top tips for users and continue to build them throughout the project.
- Consider requirements for the NHS Data Security and Protection Toolkit from the start to ensure you design compliant processes.
- Review ICO best practice for BYOD implementations.
- Review National Cyber Security Centre BYOD advice.
4. Analyse benefits and risks

You’ve thought about what you might offer via BYOD and the data involved, next you need to review the benefits you’ll get and analyse the risks. Baselining these and selecting KPIs will help you measure success once your project completes.

Benefits

- Baseline the current process and future benefits of the BYOD approach.
- Are there time, quality and cost benefits involved? BYOD has been linked to productivity gains, employee satisfaction, morale improvements, increased innovation and flexibility, employee retention and more.
- Think about how you can measure these potential benefits now and in the future.

Risks

- What are the risks involved in the proposed application of BYOD?
- Perceptions and opportunity may differ between roles impacting uptake and use of BYOD.
- Consider security risks, adoption barriers, knowledge and training challenges, costs to implement and those of ongoing administration and management.
- Review options to mitigate and manage the risks documented.

KPIs

- Identify your primary reason for implementing BYOD and decide on some key performance indicators which will help you monitor progress towards this goal.
- Useful metrics might be:
  - Number of Users / Logons / Minutes of use
  - Productivity feedback from users
  - Employee satisfaction
  - Helpdesk support impact / IT costs
  - Staff retention over time
5. Investigate technical options

Research revealed a difference in perspective on how BYOD should be implemented.

Those who had implemented BYOD mostly did it within their own teams whilst those thinking about BYOD were more varied about the best route to implement. The impact on IT support was minimal in BYOD organisations whereas to those yet to implement said it was their highest concern.

- Work with local organisations and those in a similar sector to yourself who have already successfully implemented BYOD. Don’t reinvent the wheel.
- Understand challenges faced by other organisations and heed their lessons learnt.
- Many existing NHS BYOD organisations implemented with their own staff which brings local knowledge of the Trusts existing systems, policies and culture.
- Also consider external support to bring in new ideas and help the project avoid blind spots caused by policy legacy or a lack of experience.
- Large scale rollouts have succeeded in having a low support impact and focusing on this will make the solution sustainable and cost effective.
- Look for technical systems which will provide the required controls. Most Mobile Device Management (MDM) solutions can be configured to protect data and devices without impacting personal user data. Investigate the market and test assumptions.
- Model the costs of various options and the potential savings.
- Visit organisations using different products to understand how they work in context.
- Aim to containerise BYOD apps for your employees to separate work apps from personal.
- Consider using a curated app store and ensure there is a process for employees to request updates to the list of trusted software.
6. Build policy and processes

Now you’ve determined your technical solution and data governance and you know the risks to avoid and the benefits you desire you’re set to develop your policy and processes. Research revealed that many organisations operate BYOD without any policy. Where policies were in place, often they were hard to find and difficult to understand.

Write your policy with the reader in mind. An example policy is provided alongside this guide.

- Develop a new stand-alone BYOD policy so staff know where to find the latest guidance.
- Be clear about the responsibilities on the user to maintain their device security.
- Don’t make BYOD mandatory but offer it as widely as possible.
- Assure staff about how BYOD systems are secured and what personal data might be accessible to the employer.
- Ensure the policy covers audit processes to monitor and review BYOD compliance.
- Address the issue of remuneration so that employees are clear where they stand on costs.
- Consider what happens if personal devices get damaged during work usage.
- Build a culture of trust and encourage staff to self-report issues to enable rapid resolution.
- Build processes for onboarding and offboarding of users.
- Ensure a process exists to allow staff to request apps be added to the curated app store.
- Review other policies which may reference the use of personal devices, update them to reflect the organisations BYOD approach.
- Consider whether multi-level policies would be beneficial if usage of BYOD or application access could be different based on role or position.
7. Implement

Implementation of a BYOD solution is similar to any project although there are two key areas to be aware of. Firstly, you are probably providing access to an application via a new route and this needs thorough planning and testing. Secondly, you are offering a completely new way of working to users and should recognise and respect the cultural norms you may be disrupting.

- Develop an implementation plan and consider including the following:
  - Documentation and objectives from your work so far
  - Lots of user engagement and comms
  - Procurement and solution options
  - Implementation phases and test plans
  - Technical assurance via external penetration testing
  - User training and support plan

- Rollout the chosen solution carefully and ensure comprehensive testing throughout.

- Review WiFi and network capacity where there could be high utilisation of BYOD.

- Provide training to colleagues as the solution is launched ensuring expectations are explicitly discussed such as the user need to maintain the device’s software and to report any problems.

- Roll out to support staff first so that they can familiarise themselves with how the solution works.

- Check the documentation for users and support staff is adequate.

- Work closely with colleagues to resolve issues as they occur.

- Keep your organisation updated on the plans and the progress.

- Monitor impact on work / life balance, be sure to protect staff from overwork.

- Consider how systems would be shut down or devices wiped if there were a need.
8. Monitor and review

Many organisations don’t have a BYOD policy and even those who do often don’t have a process to monitor and review compliance.

Given the concerns about data security and the potential for additional pressure on some individuals it is essential that some form of monitoring is put in place.

- Audit for compliance regularly throughout rollout and follow up on audit outcomes.
- Review benchmarks and KPIs pre and post implementation and on an ongoing basis.
- Conduct a systematic review of the project – use interviews and surveys to gain insight into how productivity and/or staff morale have been impacted.
- Identify the actual benefits and costs.
- What issues were uncovered and how were they addressed?
- What was the support impact?
- Update documentation, processes and policy at least annually.
- Remember your systems and user devices continually evolve.
- Report progress and decide to scale up if all goes to plan.
- Think about another application or use-case.