

Improving NHS Community Nursing with Mobile Technology

Recommendations for success

White Paper



Bittium

Improving NHS community nursing with mobile technology - recommendations for success
White Paper

Copyright 2018 Bittium. All rights reserved. The information contained herein is subject to change without notice. Bittium retains ownership of and all other rights to the material expressed in this document. Any reproduction of the content of this document without prior written permission from Bittium is prohibited.

Table of Contents

1.	Introduction	4
2.	Key observations.....	5
2.1	Ease of use.....	5
2.2	Connectivity	5
2.3	Network coverage	5
2.4	Application behaviour.....	6
2.5	Security.....	6
2.6	Development, integration and roll-out	6
2.7	Cost efficiency.....	7
2.8	Measure, analyze and adapt.....	7
2.9	Fit for purpose.....	7
3.	Conclusions.....	8
4.	Bittium SafeMove®	9

1. Introduction

With the recent publication of the “Next Steps on the NHS Five Year Forward View”, the government has laid down its plans to invest in new technologies to improve health provision and go paperless by 2020. Factors such as a growing and aging population, combined with a lack of hospital beds, have resulted in more emphasis being placed on treating patients in the home. Digitalization has the potential to revolutionize the health service and the introduction of technology including mobile devices using wireless networks in a community setting promises to greatly improve how services are provided. For example, being able to directly update a patient record during a home visit, or view accurate and up to date prescription history with the patient are key to improving outcomes.

The introduction of mobile technology to community nursing however is not without its challenges.

A recent report by the Queens Nursing Institute (QNI) published in April 2018 entitled “Nursing in the Digital Age – Using

*technology to support patients in the home”*¹ surveyed 534 community health professionals to find out how they are responding to the new digital agenda. Whilst recognizing the potential advantages of digitalization, community nurses were also keen to point out the barriers to adoption, highlighting that the systems they are using have not generally been tailored for community nursing; and that poor connectivity results in mobile applications behaving unreliably or not at all.

Based on Bittium’s real world experience serving as a wireless network specialist and connectivity software provider for the NHS, and in particular the successful implementation of mobile technology for several community care teams at Trusts throughout the UK, this whitepaper outlines some key technical considerations that are crucial to the success of mobile working projects in the NHS and provides some recommendations for success.

“Poor connectivity hinders efficient ways of mobile working. A lack of and/or limited connectivity means that some systems do not update, synchronise or function. This leads to nurses spending time duplicating information as paper records are transferred onto systems back at base.”

“Nursing in the Digital Age– Using technology to support patients in the home”
Report by The Queen’s Nursing Institute, 2018

2. Key Observations

2.1 Ease of use

Community nurses provide a vital role in care provision but they are not necessarily trained in modern IT. The introduction of laptops and tablets to their daily routine can introduce additional complexity which can interfere with care provision. The new requirement to boot the laptop, logon to Windows, check connectivity, log on to the VPN using tokens, run key applications, record medical notes via the keyboard, and deal with poor or lost connections to avoid losing work whilst providing much needed medical advice can prove impractical. Difficult to use systems lead to less time with patients and any anticipated efficiency gains are quickly lost. Poor user experience can lead to workers reverting to pen and paper and causes whole mobility projects to fail. We need to deliver technology that automates the experience where possible; is delightful to use; and have technology serve the user and not the other way around. Mobile computing equipment and software applications must be seen as tools for health care workers to perform their primary tasks with less effort and more efficiency, and not as a burden by adding new tasks and obligations.

Recommendations:

- If possible, choose connectivity management software that runs automatically on device startup, selects the best network, connects the VPN and keeps the device securely connected to the best available mobile, Wi-Fi or wired connection at all times.
- Avoid complicated network logon steps by selecting remote access or VPN software that uses Public Key Infrastructure (PKI) certificates for authentication at the device level, allowing encrypted connections and reconnections after a network break to be renewed automatically and not require user involvement.
- Ensure Windows requires secure logon and protect Windows passwords, perhaps with two factor authentication.

2.2 Connectivity

Improving network connectivity, especially at the point of care, is the single technical measure with the greatest positive effect on performance, efficiency and user experience for mobile health workers. Poor network signals or low bandwidth can result in significant frustration. Erratic application behavior can lead to work being lost and connections needing to be reestablished. Automatic configuration and management of network parameters and interfaces is a must. Mobile Virtual Private Networks (VPN) and connection management software can

help to automatically connect, and keep the device connected to the best available network. They can also offer session persistence to keep applications running during periods of poor or no connectivity, and seamlessly switch between networks without user intervention when they become available further improving the user experience.

Recommendations:

- Avoid interrupted sessions by using software that implements "session persistence" allowing applications to pause rather than break when network connectivity is intermittent.
- Utilize software that seamlessly and automatically switches between mobile, Wi-Fi and wired networks allowing applications run smoothly whilst taking advantage of the best available networks over time.

2.3 Network coverage

Closely related to connectivity, actual network coverage has a major impact on mobile working performance and the ultimate success of a mobility project. Mobile 4G (LTE) network coverage is already adequate in densely populated areas and continues to improve. This is an enabling factor, but will not be enough on its own to provide sufficient coverage for all health care applications which are typically needed in less populated urban or rural settings. Choose the right mobile technology and the operator with the best coverage for your users specifically. Complement mobile coverage with public and private Wi-Fi. Security risks associated with the use of public Wi-Fi services can be overcome by using appropriate VPN and firewall technology with built-in hotspot landing page or automated hotspot access capability. Complementing mobile data with such a WiFi service can significantly improve coverage and network speeds especially in rural environments. Software to allow seamless transition between mobile and Wi-Fi networks is recommended for the best user experience. The use of home broadband and also smartphone tethering can also be used to boost coverage.

Recommendations:

- Verify which public and private Wi-Fi services are available in your community. Study coverage maps provided by the operator, or better still, utilise connectivity analytics software to achieve this.
- Complement mobile data coverage with Wi-Fi hotspots. Major public Wi-Fi networks available in the UK include

BTWi-Fi (BT), The Cloud (Sky) and o2wifi (O2). The BT service for example, allows access to over 5 million Wi-Fi residential home hubs through the BTWi-Fi FON service.

- Explore guest Wi-Fi services and those provided by schools, hospitals, social services etc which may provide NHS access. Govroam is an example of this.
- Where possible, automate the provisioning of Wi-Fi networks and keys automatically so that users do not need to add them manually.

2.4 Application behaviour

How do your applications behave in different network conditions? Some applications support an offline mode, while others require a constant connection to operate. Many legacy health-care applications designed for the desktop were not written with mobile use in mind and may fail or require restarting when network disconnects occur. This may result in data entered being lost and needing to be re-input. All applications however benefit from improved connectivity and coverage. Know and test your applications and build a platform that provides sufficient connectivity and seamlessness.

Recommendations:

- Verify that applications can operate with low bandwidth, high latency intermittent connectivity without losing data.
- Where available, move to offline versions of the application software which do not require a permanent connection to operate and connect when available to exchange data.
- When a permanent connection is required, such as when using remote desktop services, implement a connectivity platform that hides the temporary gaps in connectivity from the service, allowing it to pause during periods of short connection breaks rather than hang.
- Consider incorporating public Wi-Fi services such as the BTWi-Fi network available in over 5 million residential homes across the UK.
- Look for possibilities to improve network coverage also away from the home by for example by utilizing guest or hospital Wi-Fi networks. If connectivity analytics software is available, look at the available networks broadcasting in the area.

2.5 Security

NHS Healthcare applications and networks have clear data security requirements. For mobile working, strong network security is a must, but also protection of data stored on the device. Device tracking and remote management are also important. Take care not to sacrifice usability for the sake of security. VPNs not designed for mobile use often perform poorly. Secu-

urity must be always-on and work with as little user intervention as possible. Stay away from solutions that only protect a single application. Instead use network security that protects all network traffic and use full disk encryption. For example, consider using a VPN to connect your mobile devices to the Trust's own network with all existing services including HSCN/N3 hosted, instead of limiting your applications to only N3/HSCN services by terminating the VPN to an N3/HSCN provider.

Recommendations:

- Use a standards based (e.g. IPsec) VPN specifically designed for the mobile environment that does not require constant user actions to operate.
- To ensure the best ease of use, use PKI device certificates to automatically authenticate device network access; and use two factor authentication (e.g. smartcard) to access sensitive applications.
- On Windows, allow the device to logon to the VPN automatically during startup and before the windows logon appears. This will allow critical updates to be downloaded automatically, including password resets etc, and allows lost or stolen devices to be disabled or deleted.
- Use a VPN for security that encrypts and protects *all* traffic base on policy, rather than rely on application specific security (such as SSL) alone.
- Always use full disk encryption to protect the data at rest.
- Connect the VPN to the Trust and from there allow access to Trust and N3/HSCN services.
- Enforce strong passwords and ensure passwords are correctly managed.

2.6 Development, integration and roll-out

A mobile application, such as a health care data entry system, can require that a great many components work perfectly together before it can be successfully used or even tested. For example, mobile hardware, new application software, connectivity, security, servers, and integration with existing infrastructure all need to be in place. This complexity often leads to protracted implementation projects and extended trial iterations. Consider a more agile project approach where real value and new benefits are delivered early on and in stages. For example, set up access to the trust email or some other existing applications at an early stage so that users can benefit from the mobile equipment even before a new mobile application is ready and integrated. In this way the different components can be evaluated more independently, leading to earlier feedback and better results.

Recommendations:

- Allow time for users to become acquainted with the new technology. Allow access to general apps on the device, such as email or Skype for Business etc, at an early stage rather than releasing the complete mobile system on one hit.

2.7 Cost efficiency

Mobile technology and mobile working practices promise increased operational efficiency and cost savings. However, quality mobile equipment is expensive and there are recurring costs such as mobile data plans. Better cost efficiency can often be achieved by selecting a general purpose connectivity and security platform with a planned, ongoing life cycle, instead of building a one-off system to serve a single mobile application. This way the same equipment and infrastructure can be fully utilised for existing, planned and future applications with a clear upgrade path. Connectivity software with filtering and monitoring can be utilised to optimize network usage to eliminate unnecessary cellular data transfer and reduce costs of data plans.

Recommendations:

- Select a platform that will protect and optimize *all* network traffic rather than just secure traffic for one application. Ensure that the platform suits your future needs, for example, by supporting other mobile platforms and operating systems.

2.8 Measure, analyse and adapt

Ultimately, the success of a mobile working project is measured by improved patient outcomes, increased efficiency and cost savings, e.g., in the form of reduced referrals and fewer hospital admissions. This however will not be realised until the system has been fully operational for some time, and it will be difficult to discern how much truly can be attributed to new mobile working practices. In order to reliably achieve the objectives, the performance of the technical elements and of the mobile working processes themselves need to be gauged throughout the project – from early development into production. The capacity to measure, analyse and quickly adapt is crucial. Be prepared to answer questions such as: Which users are using the application as intended, i.e., wirelessly away from home or the surgery? Where are the devices being used? What percentage of time do our devices have sufficient connectivity? What percentage of work shift time are the devices switched on? Which mobile operator provides the best coverage for our users?

Recommendations:

- Make use of **connectivity and device analytics software** to allow objective measurements of overall system performance to be made. This combined with subjective feedback from end users can provide a more evidence based appraisal of how the new technology is being adopted.
- Understand if mobile devices are being used away from home or the Trust networks.

2.8 Fit for purpose

The choice of device type is critical for the adoption of mobile applications. If the end users are not happy with the form factor (laptop, tablet, iPad, phone etc.) they may revert to pen and paper and the expected benefits of the digital investment will not be realized. The QNI study revealed that laptops are used more frequently compared to compact devices such as tablets, iPads and smartphones, although some found that the laptops used were considered heavy, slow, outdated and cumbersome. Connectivity on laptops was perceived to be a challenge and in some cases Wi-Fi networks were not being utilized back at base. Tablets and iPads on the other hand were considered to be expensive and unsuitable due to the small screens and difficulties inputting information along with causing neck and eye strain with some users.

Recommendations:

- Test the devices with the users prior to roll out.

3. Conclusions

At Bittium, we have had the privilege to take part in several mobility projects with NHS Trusts, such as the Staffordshire and Stoke-on-Trent Partnership NHS Trust, and Rotherham Foundation Trust. As a conclusion, we would like to share some details on decisions and actions that were taken in these projects, that we find have contributed to their success.

In the projects we took a platform approach to security, mobility and application delivery. The Trusts decided to use a general purpose Windows laptop or tablet as part of their existing Microsoft Windows domain. A benefit of this choice is that it can support any existing legacy services, such as expense claim system in addition to planned, dedicated mobile working applications and any future software applications.

The laptops and tablets were equipped with the **Bittium SafeMove® Mobile VPN** client in order to meet the high usability and security requirements we had set. The most important functionality we implemented was:

- An always-on, secure VPN connection to the Trust's internal network is established and maintained without requiring any action from the user. Over this connection, services such as N3 can be accessed, but any other services used by the Trust can also be made available.
- Seamless switching between networks and session persistence that enhances connectivity for all applications
- Seamless utilization of public Wi-Fi networks available at homes in the community such as BT WiFi-with-FON in order to amend cellular network coverage and improve connectivity

In order to accurately measure success and identify problems and their root causes the team, together with NHS Trust IT and clinical personnel, developed a process to collect data relating to connectivity and mobile device usage and to analyse it. We found this to be very useful for several different purposes:

- Measuring connectivity performance
- As a basis for choosing between options such as cellular operators and public Wi-Fi networks
- As a basis for making investment decisions on technology such as personal hotspot devices (3G/4G pocket routers) and public Wi-Fi contracts, with the objective of increasing network coverage
- Assessing how well the intended Community Care mobile working process is applied, by analysing data on where and when the devices have been switched on, and to what networks they have been connected.

4. Bittium SafeMove® Mobile VPN

Bittium SafeMove® is a software product family for secure, mobile connectivity with focus on mobile working in NHS organizations and field engineers at utility companies in the UK.

Bittium SafeMove® offers:

- An always-on, mobile VPN
- Automatic connection management, with seamless network switching
- Network session persistence
- Fully automatic and seamless utilization of public Wi-Fi networks such as BT-Fon
- Analytics - an extensible data collection and analysis tool
- Experience in working with NHS requirements and integration with NHS infrastructure, such as the NHS smart card.
- Unparalleled user experience

For more information about Bittium SafeMove® solutions and how we can help to improve the efficiency of your mobile care workers, please visit our website www.bittium.com or contact our sales at safemove.sales@bittium.com.



