iCleanse

BYOD

Is Disinfection Part of Your BYOD Policy?

The use of mobile technology in the healthcare setting continues to rise.

Choosing the option that makes the most sense for your company will depend on the sensitivity of your corporate data and your pre-existing policies.

A recent survey conducted by Epocrates found that 86% of clinicians are using their smartphones for professional activities, 53% of those clinicians are also using tablets.

That same survey estimates that 9 out of 10 medical professionals will be using both tablets and smartphones for professional purposes by the end of 2014 (Epocrates, 2013).

As the adoption of tablets and other mobile devices in healthcare continues to rise, employers need to determine the most ideal method of implementation. When it comes to deploying tablets in a clinical environment, hospitals have three main options:

1. Provide a pool of the tablets to be shared within the workplace.

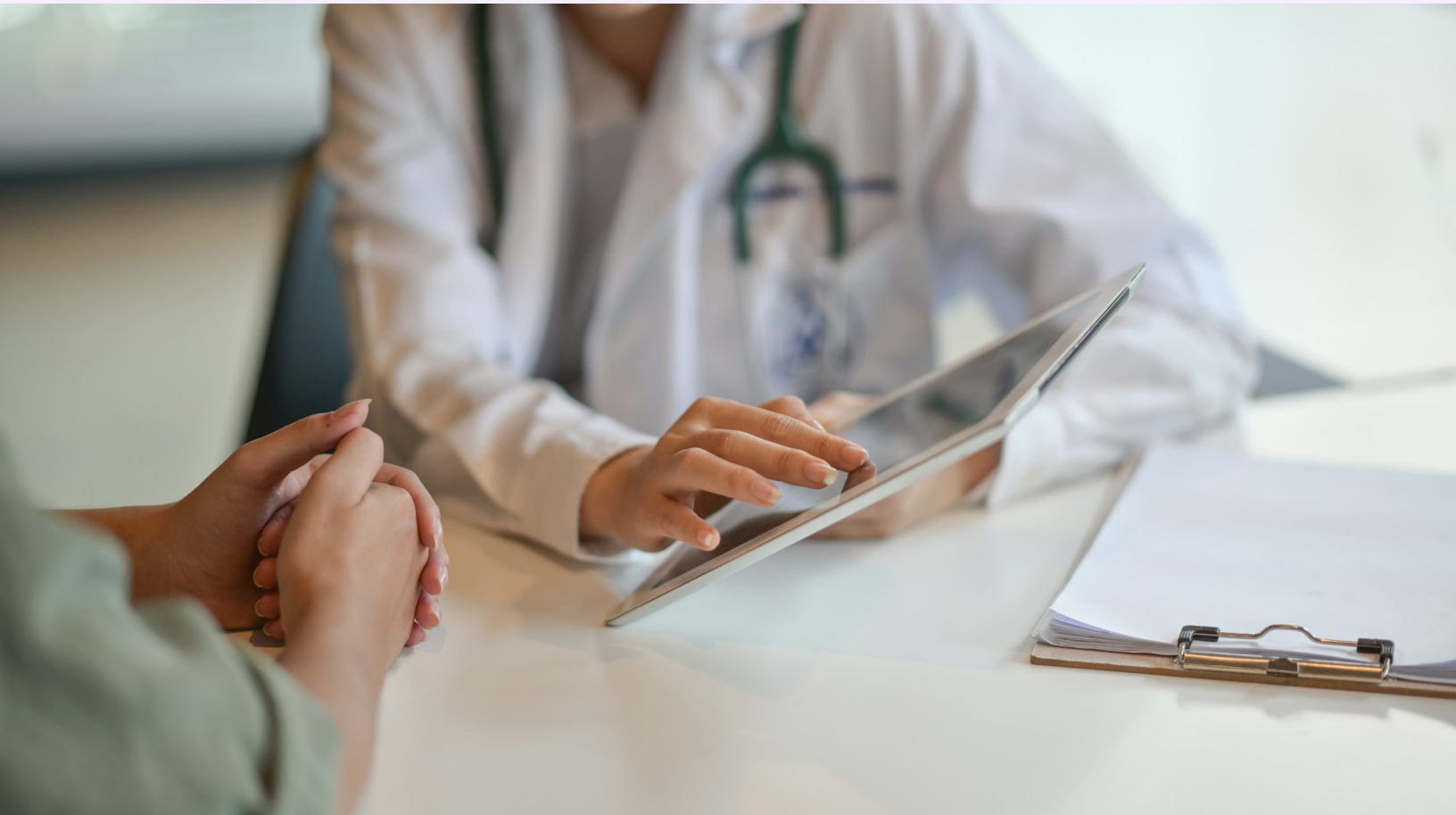
2. Provide corporate-owned personally-enabled (COPE) device.

3. Support a bring-your-own device (BYOD) methodology.

At this point in time, BYOD appears to be the most popular choice among hospitals.

A recent survey conducted by Aruba Networks reported that of hospital-based IT professionals claim that their organization employs a BYOD strategy (iHealth Beat, 2012).

While BYOD certainly offers a lot of convenience for employees, there are many things that hospitals need to consider prior to introducing such a policy.



What to Consider When Developing a BYOD Policy for Tablets & Mobile Devices

Security

Likely the most important consideration prior to implementing tablets in a healthcare setting is security. Many healthcare professionals have concerns about private patient data walking in and out of the office on a regular basis. The inability to constantly monitor these mobile devices leads to a higher risk of theft, especially since many users do not have password protection on their tablets.

Managing this security concern also raises another issue around balancing company monitoring of personal property and maintaining healthy employment relationships. Developing a system to monitor or control the use of an employee's personal device requires the company to walk a fine line between patient security and rights of ownership. Patient confidentiality is mutually understood between clinicians and employers, but the means of maintaining that confidentiality is a bit of a gray area.

A company's ability to manage sensitive data within a BYOD policy is critical to reducing the risk of a potential breach. Without a central management system, employers would find it difficult if not impossible to assess any potential data breaches from a compromised device.

Moreover, if a BYOD user is able to bypass corporate controls, their mobile devices may become susceptible to viruses and malware that could ultimately expose secure patient data (Phifer, 2013).

The Digital Services Advisory Group and Federal Chief Information Officers Council have attempted to address this issue by outlining three high-level means of managing BYOD security (Digital Government, 2012):

Virtualization: Put all computing resources in a centralized cloud system so that no data or corporate application processing is stored on a personal device.

Walled Garden: Locate all data or corporate application processing within a corporate controlled application on the personal device.

Limited Separation: Allow both personal data and corporate data to be accessed on a personal device with security policies in place to ensure that information controls are satisfied.

These three options all offer different levels of security. Choosing the option that makes the most sense for your company will depend on the sensitivity of your corporate data and your preexisting policies. Regardless of the option you take, managing security is a critical element of implementing tablets into your workplace.

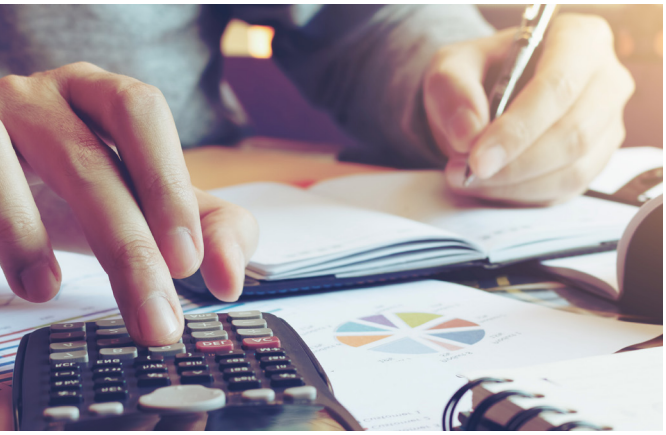
Cost

When it comes down to the cost of implementing tablets into a work environment, many see BYOD initiatives as a way to reduce costs. While BYOD policies help to reduce the start up costs associated with purchasing these mobile devices, there are a variety of associated costs that many decision makers do not consider.

Employees need empowerment to be able to use their devices freely which brings about a variety of costs. Dr. Gary Woodill, senior analyst from Float Mobile Learning highlights the three main challenges associated with wireless services charges from BYOD networks (Freifeld, 2013).

Employee Compensation: Many employees will look to be reimbursed for the portions of their bills that were associated with company activities. This can be handled in a variety of ways, including a stipend approach, but heavy usage or business-related roaming charges can quickly send this bill skyrocketing.

Handling Additional Expense Reports: When managing the cost of these BYOD devices, companies will need to establish a system for monitoring wireless expenses. This either requires upgraded software or additional hours to complete, further boosting operating expenses.



Unqualified for Service Discounts: When a company is looking to set up a group service and data plan they have the power to negotiate a discount for bulk service provision. A BYOD policy leaves employees responsible for their own data plans, and removes the company's power to receive any discount for business-related charges.

Additional costs will also come into play during the initial implementation of a BYOD policy. IT will be responsible for ensuring that employees have access (or lack thereof) to the correct information, which will result in many hours of labor for policy planning and plan development.

Current estimates vary in the actual cost of a BYOD policy due to the nature of implementation strategies.

Overall, Garter estimates that BYOD policies cost enterprises $100 per employee annually to $300 and expect this number to triple by 2016.

This number certainly varies by company due to policies that determine levels of information access and reimbursement (Donovan, 2013). Many companies choose not to provide reimbursement for BYOD initiatives, but this opens up other questions about employee satisfaction and long term implications.

Policy

The effectiveness of a BYOD initiative lies in the ability to develop asecure, flawless, and uniform user experience. Users need to be ableto access the appropriate information from wherever they are working.In order to do this, there are a variety of choices that need to be madefrom a policy standpoint. These areas include:

Approved Devices/Applications

Businesses need to clearly communicate exactly which devices will be usable within the established BYOD policy. Ideally all devices will be able to provide a consistent user experience, but complications in policy development may create restrictions on device usage. Certainlythis may contradict the idea of bringing your own device if certain devices are excluded (i.e. a strictly iOS policy), but it is acceptable as long as employees are informed in advance.

Policy developers will also need to consider the third party applications that employees will be able to access under the BYOD policy. Certain applications that share a large amount of data may compromise the security considerations of a BYOD policy. It is key for policy makers to identify a list of popular applications/types of applications that will be allowed/banned.

Data Ownership

Data ownership is an easy consideration on the surface – companies own the data that employees are accessing on internal servers, and in many cases this information is legally protected (i.e. patient records). The issue arises when a device is compromised in some way (stolen, hacked, etc..) and needs to be remotely wiped. A traditional wipe will remove all data on the phone, including potentially irreplaceable personal data such as pictures and music (Hassell, 2012). When developing policies, it is wise to establish a system to backup this information on a regular basis to ensure that this problem does not arise.

Device Support

Employees will want to know what support is available from the internal IT department. Policies must be developed to determine what happens in the event that a device is broken on site. A policy for training and maintenance will also need to be clearly outlined to establish the procedure to provide these services efficiently from both a cost and operational standpoint.

Permitted Use

A thorough BYOD policy will need to outline exactly who is permitted to use devices and where. In clinical environments, Infection Control will need to become involved to establish, at the very minimum, where these devices can be used so that physicians and patients are not transferring germs on the surfaces of these devices (disinfection policies can help to break down some of these barriers).

Managing the staff usage of these devices is one thing, but what happens if a patient or guest want to bring their own device? Tablets and other mobile devices can go a long way

in helping to keep patients and other guests comfortable, informed, and directly engaged in their care, so including these groups in a BYOD initiative can help to improve overall patient care. Again, Infection Control will need to be involved to determine usage restrictions and disinfection policies, but as mobile device adoption continues to increase this could become a crucial area of BYOD policies.

Remote Access

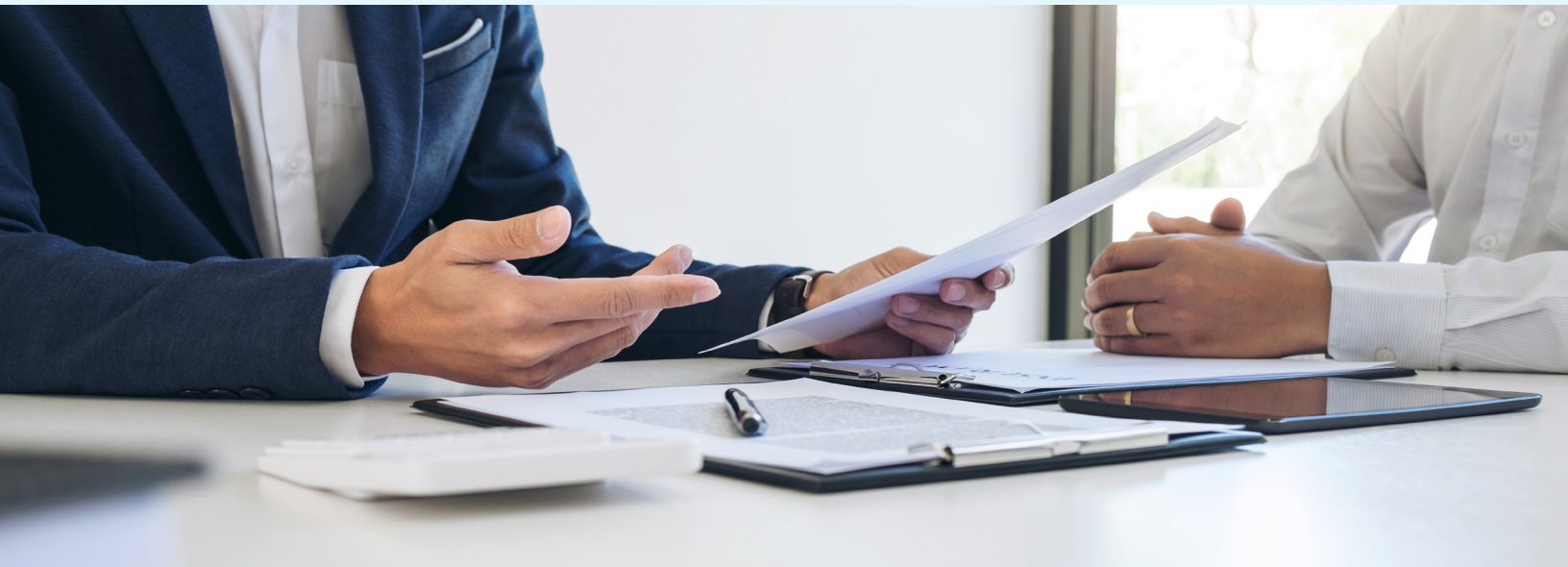
A BYOD policy is effective for employees within the walls of the hospital or office. However, when a clinician needs to travel or a hospital needs to host a visiting doctor, will they truly be able to bring their own device?

For traveling doctors, most third party applications can be accessed from anywhere, but access to your internal network could be a potential security threat. Traveling clinicians can be given access to the network remotely via a VPN, but even that is not without its risks. Hospitals will need to determine the best course of action for their own personal network, based on the framework of the overall security plans.

Similarly, for those hospitals that are hosting visiting clinicians the decision will need to be made whether or not these guests should be given access to the internal network. In most cases guest access can be granted, but the initial setup time may be viewed as a hassle for both parties. An established BYOD policy should help hospital networks that frequently work together determine the best course of action for empowering their employees and visiting staff to effectively perform their duties.

Exit Strategy

When dealing with personal devices, an exit strategy is one of the most key components of security. Your BYOD policy should have a plan in place to quickly remove access to the network, email, and confidential information with minimal impact on personal data. The easiest way to execute an exit strategy is to have employees routinely back up their personal data so that it can be retrieved after a complete wipe of their system takes place. Other options are available, but may be more time consuming and manual, so it is best to have an exit strategy as a part of your BYOD policy from day one.



Technology

Generally the management of a BYOD program will fall on the shoulders of IT. Depending on how large of a BYOD network you have at your hospital, this task could become multiple full-time jobs. Prior to developing a BYOD program you will need to ensure that you have the necessary human resources in place. Even with the right people, managing a BYOD program can be challenging without the proper technology.

As the popularity of BYOD has continued to grow in healthcare, more players have gotten into the game of creating mobile device management systems (MDM) or enterprise device management system (EDM). The technology that you choose will go a long way in determining how much pressure is put on the IT staff to keep things running smoothly.

Some of the most popular MDM systems on the market today are listed above. An thorough review of your expectations from this technology should help to determine the best option for your network.

Disinfection

Many of the elements that have been covered thusfar seem like obvious concerns for a BYOD policy. Developing a clear road map that outlines a secure, cost-efficient plan is the heart of any major implementation. However, there is still one critical element that is often overlooked when creating these implementation plans: disinfection.

It is certainly not a lack of emphasis on the importance of disinfection that causes this element to be overlooked. Hospitals and other healthcare environments understand the importance of disinfecting high-touch surfaces used by both patients and staff. Rather, the novelty of using tablets and other mobile devices in the workplace has created uncharted territory for Infection Control.

We tend to use our cell phones, tablets, and similar mobile devices on a daily basis without even considering the bacteria that may be present on the surface. Average users don't even think of cleaning or disinfecting their device on a regular basis because the surface looks visibly safe. However, studies have shown that the screen of a cell phone contains 18x the bacteria of an average toilet seat.

Moreover, the screens on cell phones and other mobile devices offer germs a reservoir to linger for days, weeks, or even months. What is most concerning is that many of the top ten most common pathogens that account for over 80% of the hospital acquired infections in the US are also among the organisms capable of surviving the longest on surfaces. For those with susceptible immune systems, simply coming into contact with a screen harboring certain bacteria could result in devastating consequences.

In the case of BYOD, the implications of lingering pathogens extends outside of the walls of the hospital. According to a 2013 study by JD Power & Associates, 51 percent of tablet owners share their devices with at least one other person (Arlotta, 2012). While many see this as a potential security risk, it can be a severe health risk. Doctors and nurses can easily and unknowingly transfer dangerous germs back and forth between work and home, exposing both families and patients to potentially harmful bacteria (Sittig & Ash, 2009).

Mobile devices are only recently being recognized as roaming high-touch surfaces, and thus require frequent disinfection between uses. Typically this involves wiping down the device with a chemical disinfectant, which is not without its complications. In order for these wipes to deliver true disinfection, all on-label instructions must be adhered to (Rutala & Weber & HICPAC, 2008). Failure to do so can leave the hospital liable for any potential complications that can be traced back to the device (Garrett, 2011). Beyond that, the use of chemicals on these devices automatically voids most manufacturer warranties.

So how can you work disinfection into your BYOD policy?

There are two main options at this point in time that will ensure your tablets and other mobile devices are disinfected to a level that is safe for human contact: chemicals and germicidal light.

Chemical disinfection is an effective means of disinfecting most hospital surfaces, but it does not come without some of the complications outlined above. However, with proper precautions (i.e. allowing proper exposure time), this method can be an effective means of keeping both patients and caregivers safe. A newer option that is gaining in popularity is the use of germicidal light to deactivate the bacteria on the surface of these devices. Docking stations and room scanners are being developed to bathe mobile devices with an appropriate dose of light.

Regardless of the method you choose to disinfect your mobile devices, it is important to make sure that it is a documented part of your policy. Routinely disinfecting these roaming high-touch surfaces will ensure that patients, doctors, nurses, and all of their families are safe when using these devices – for work or play.

Takeaway

Allowing healthcare professionals to bring their own devices to work has helped many hospitals to increase their overall efficiency. The number of uses for these devices is growing daily, and it does not appear that this trend will fade anytime soon. As these new technologies continue to be adapted into these germ-sensitive environments, proper policies need to be developed and continually updated to ensure a safe, secure, and efficient operational process.

References

Arlotta , C. (2013, April 29). Byod v. cope: Can either model address sharing device?. Retrieved from http://mspmentor.net/mobile-device-management/byod-v-cope-can-either-model-addresssharing-device

Digital Government. (2012, August 23). Bring your own device. Retrieved from http://www.whitehouse.gov/digitalgov/bring-your-own-device

Donovan, F. (2013, May 5). Per-employee cost of byod will triple by 2016, predicts gartner read more: Per-employee cost of byod will triple by 2016, predicts gartner - fiercemobileit http://www.fiercemobileit.com/story/employee-cost-byod-will-triple-2016-predictsgartner/ 2013-05-05

Epocrates. (2013). 2013 mobile trends report. Retrieved from http://www.epocrates.com/oldsite/statistics/2013 Epocrates Mobile Trends Report_FINAL.pdf Freifeld, L. (2013). To byod or not to byod. Retrieved from http://www.trainingmag.com/content/byod-or-not-byod

Garrett, J. H. (2011, September 20). Making sense of disinfectant labels: A step-by-step approach. Retrieved from http://www.infectioncontroltoday.com/articles/2011/09/making-sense-of-disinfectant-labels-astep- by-step-approach.aspx

Hassell, J. (2012, May 17). 7 tips for establishing a successful byod policy. Retrieved from http://www.cio.com/article/706560/7_Tips_for_Establishing_a_Successful_BYOD_Policy?page=2&taxonomyId=600013