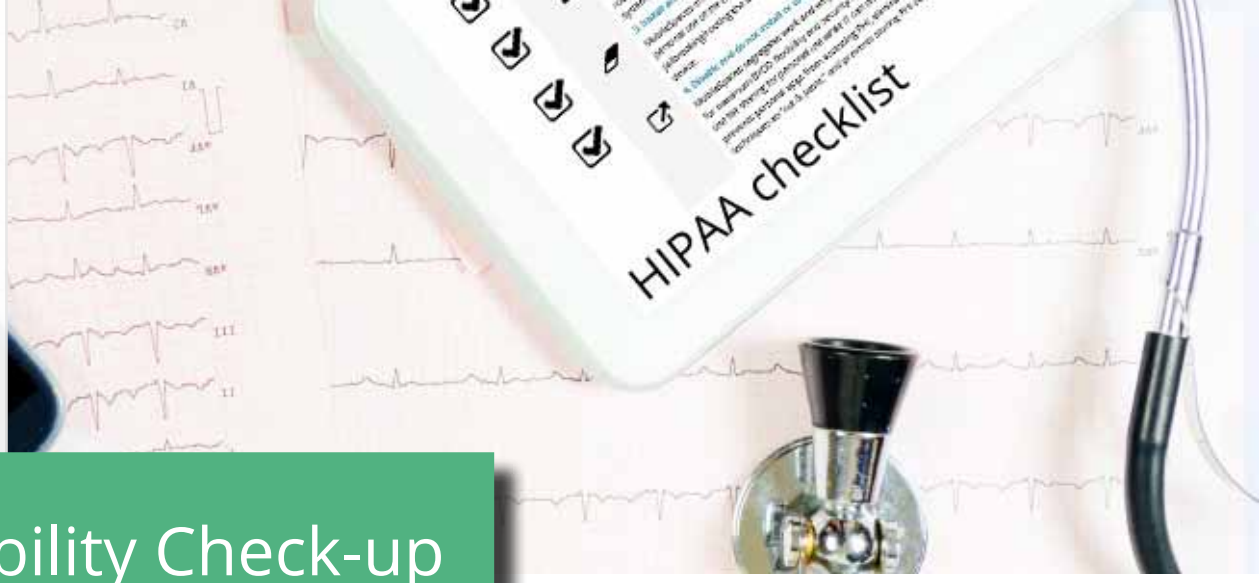
mobile spaces



HIPAA Mobility Check-up

The 2013 deadline for the HIPAA Omnibus Rule has come and gone. Have you secured your mobile users?

Security with simplicity — that's how MobileSpaces allows you to quickly secure protected healthcare information (PHI) in a BYOD world. Our container-security and mobile application management creates a trusted workspace that provides strong HIPAA security for both Android and iOS devices while also simplifying the administration of healthcare mobile apps. The workspace secures PHI against data leakage and loss by encrypting all data at rest, controlling data sharing between mobile apps and connecting directly to your VPN. You can fill the workspace with any mobile app, whether it be from the public app store, customized or built-in; everything is easily cloud-managed with policies controlled from a browser-based console.

Compliance with the HIPAA Security Rule is simple with MobileSpaces. To show you how, we have mapped our features to this government checklist for mobile device privacy and security.

1. Use a password or other user authentication.

MobileSpaces supports a policy-based passcode or pin on the workspace or mobile device. Policies include passcode complexity, history, inactivity timeout, and penalty enterprise wipe for max tries.

2. Install and enable encryption.

MobileSpaces provides an encrypted workspace that protects PHI on a personally-owned iOS or Android device. MobileSpaces also verifies that the device is not jailbroken or rooted to ensure that the inherent data protection capabilities of the mobile operating system have not been compromised.

3. Install and activate remote wiping and / or remote disabling

MobileSpaces enables IT to remotely lock or wipe the workspace without affecting personal use of the device. In addition, wipes can also be used to enforce policies against jailbreaking/rooting the device or exceeding the maximum tries to unlock a workspace or device.

4. Disable and do not install or use file sharing applications

MobileSpaces segregates work and employee data, apps, communications and networking for maximum BYOD flexibility and security. Complete separation allows employees to use file sharing for personal use while IT can disable its use for work. This approach also prevents personal apps from accessing PHI, eliminates data sharing via such common techniques as "cut & paste," and prevents storing PHI outside of the workspace.

5. Install and enable a firewall

MobileSpaces uses per-app VPN to connect healthcare apps directly over an authorized connection to your existing network without disrupting how users communicate personally.

6. Install and enable security software

The MobileSpaces workspace serves as a security container that protects against malware by controlling data sharing between mobile apps and preventing unauthorized access to healthcare information and resources. The iOS and Android operating systems are designed to eliminate the security flaws of laptop technology, which required the need for malware protection. MobileSpaces ensures that these inherent protections are not compromised by monitoring for jailbroken and rooted devices and taking mitigating actions when necessary.

7. Keep your security software up to date

MobileSpaces is a cloud-based service that simplifies deployment, scale and maintenance of your mobile environment. This software as a service approach ensures that your infrastructure always has the latest security protections and tools in place.

8. Research mobile applications (apps) before downloading

MobileSpaces put IT in control. Only those applications that IT deems as trusted can be associated with the workspace. Applications can be assigned by group policy to simplify the security and deployment of healthcare apps while also providing healthcare workers with the apps they need for their job function. All apps within the workspace are controlled by IT policies, which dictate how healthcare information is stored, shared and transmitted.

9. Maintain physical control

The MobileSpaces console gives IT complete visibility of what devices and workspaces are accessing healthcare information and the compliance state of all user devices. While maintaining physical control of the device is essential in protecting healthcare information, MobileSpaces enables IT to mitigate situations when a device is lost or stolen including the use of tools to wipe the workspace, lock its access and verify the device's compliance with IT policy.

10. Use adequate security to send or receive health information over public Wi-Fi networks

MobileSpaces helps simplify your WiFi policy by ensuring that all connections from the workspace are authorized and secured via a workspace-based VPN.

11. Delete all stored health information before discarding or reusing the mobile device

MobileSpaces limits the distribution and use of healthcare apps and data to a workspace that provides container security. The workspace is fully separated from the employee's personal apps and data, giving IT full control of how sensitive PHI is shared and distributed without affecting the personal use of the device. When workers leave the employ of your organization, the workspace is simply wiped of all healthcare related apps, media, emails, attachments and data.