

uSked Information Brochure

80 M Street SE
Washington, DC 20003
(202) 250 - 3650

uSked & HIPAA Compliance

Updated August 4, 2016

Product Overview

uSked is a scheduling and logistical management system that gives a service coordinator the ability to seamlessly manage tens of thousands of hours of services a year.



HIPAA

HIPAA is the acronym for the Health Insurance Portability and Accountability Act that was passed by Congress in 1996.

Protection and Confidential Handling of Health Information

The HIPAA Privacy regulations require health care providers and organizations, as well as their business associates, develop and follow procedures that ensure the confidentiality and security of protected health information (PHI) when it is

transferred, received, handled, or shared. This applies to all forms of PHI, including paper, oral, and electronic, etc. Furthermore, only the minimum health information necessary to conduct business is to be used or shared.

uSked is HIPAA Compliant

The HIPAA lays out privacy and security standards that protect the confidentiality of patient health information. In terms of web and mobile device scheduling services, the solution and security architecture must provide end-to-end encryption and access control so data in transit cannot be intercepted. We encrypt all web and mobile app traffic and our data center is HIPAA compliant, as well as SSAE-16 and Safe Harbor certified.

Details

The following table demonstrates how uSked supports HIPAA compliance based on the HIPAA Security Rule published in the Federal Register on February 20, 2003 (45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule).

HIPAA Standard	How uSked Supports the Standard
Access Control	
Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to authorized persons or software programs.	uSked does not allow anonymous access to data. Every user has to log in and every user has an assigned role which controls and restricts what data is visible to that user.
Unique User Identification: Assign a unique name and/or number for identifying and tracking user identity.	Each user has a permanent unique ID that is never reallocated to another user. This user ID is used to track and log user activity.
Emergency Access Procedure: Establish (and	Users that are assigned an internal staff role

implement as needed) procedures for obtaining necessary electronic health information during an emergency.	can access the necessary data to share with clients and service providers at any time.
Automatic Logoff: Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	The default user setting for uSked is to log the user out after approximately 20 minutes of inactivity.
Encryption and Decryption: Implement a mechanism to encrypt and decrypt electronic protected health information.	Web and mobile app network traffic is always encrypted using secure industry standard HTTPS encryption.
Audit Controls	
Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	<p>uSked employs comprehensive time stamped logging of all user activity, including all access from web and mobile devices.</p> <p>All suspicious activity is automatically recorded and sent to the system administrator.</p>
Integrity	
Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	<p>Data alteration is only possible by authenticated uSked users having a role that allows them to do so.</p> <p>It is not possible to destroy data in uSked; when a user takes action to delete data, the system flags (marks) the data as being deleted rather than actually physically deleting it. This allows any data to be fully restored.</p>
Integrity Mechanism	
Mechanism to authenticate electronic protected health information.	Mobile device apps are digitally signed. Web and mobile device network traffic is protected

	<p>against XSS attacks.</p> <p>The uSked code and system has been tested and passed the IBM Security AppScan tool as well as tested and passed the Tenable Network Nessus Vulnerability Scanner tool.</p>
Person or Entity Authentication	
<p>Verify that the person or entity seeking access is the one claimed.</p>	<p>All web and mobile app access requires the user to log in.</p> <p>At our data center, physical access is strictly controlled by electronic perimeter access card system, CCTV security cameras, and entrances secured by mantraps with interlocking doors.</p>

HIPAA Certification

Currently, the agencies tasked with certifying health technology – the Office of the National Coordinator for Health Information Technology and the National Institute of Standards and Technology – do “not assume the task of certifying software and off-the-shelf products” (p. 8352 of the Security Rule) nor accredit independent agencies to do the HIPAA certifications. Additionally, the HITECH Act only provides for testing and certification of Electronic Health Records (EHR) programs and modules. Thus, as uSked is not an EHR software or module, our type of technology is not certifiable by these unregulated agencies.