

# VA Mobile Health: What You Need to Know about Security and Privacy

**VA Connected Care Discussion Series**  
**April 29, 2020**

Christina M. Armstrong, Ph.D.  
Clinical Psychologist, Implementation Strategies  
Office of Connected Care (OCC)  
U.S. Department of Veterans Affairs  
[Christina.Armstrong@va.gov](mailto:Christina.Armstrong@va.gov)

Beth K. Jaworski, Ph.D.  
Social Psychologist, Health Science Specialist  
National Center for PTSD, Dissemination & Training  
U.S. Department of Veterans Affairs  
[Beth.Jaworski@va.gov](mailto:Beth.Jaworski@va.gov)



**U.S. Department of Veterans Affairs**  
Veterans Health Administration  
Office of Connected Care



# Disclaimer

The following lecture is for internal U.S. Department of Veterans Affairs (VA) educational purposes.

The views expressed are those of the authors and do not reflect the official policy or position of the VA or the U.S. Government.

The authors have no relevant financial relationships to disclose.

References in this training to any specific commercial product, process, or service, or the use of any trade, firm or corporation name is for the information and convenience of the training attendees, and does not constitute endorsement, recommendation, or favoring by the VA.



# Bio: Christina Armstrong, Ph.D.



- Clinical Psychologist
- Previous: Connected Health Education and Training Program Lead, Defense Health Agency, US Dept of Defense
- Current: Connected Health Implementation Strategies, Office of Connected Care (OCC), US Dept of Veterans Affairs



# Bio: Beth Jaworski, Ph.D.



- Social Psychologist
- Previous: Research Scientist, California Department of Public Health
- Current: Mobile Apps Specialist, National Center for PTSD - Dissemination & Training Division



# Learning Objectives

- Describing how VA's suite of mobile apps handle data privacy and security.
- Addressing common questions and concerns regarding security and privacy using mobile apps.
- Explaining in plain language how apps handle data in the VA.



# Additional Training Recommendations

This training is intended to support VA health care staff on understanding and discussing security and privacy issues of mobile health apps with their patients. This training does not cover other related ethical and legal issues related to security and privacy in mobile apps and other virtual care tools. These additional TMS trainings could provide supplemental information on security and privacy:

VA Talent Management System (TMS) 2.0 (online, on demand CEU trainings)

<https://www.tms.va.gov/SecureAuth35/SecureAuth.aspx?ACTIVEX=no>

VA Mobile Training – Security of apps on iOS (VA 3926744)

Securing Mobile Devices in the Enterprise: Mobile Security (NFED 4500866)

VA Privacy and HIPAA training (NFED 4201853)

Basic Troubleshooting Techniques for Mobile Devices (VA 3936808)

Integrating National Center for PTSD (NCPTSD) Mobile Apps into Veteran Mental Health Care (VA 40943)



A close-up photograph of a brass padlock with the word "GUARD" embossed in a decorative frame. The padlock is attached to a metal shackle, which is part of a larger metal mechanism, possibly a door latch or a heavy-duty lock. The background is dark and textured.

## **Security and Privacy Issues**





Policies, Guidelines & Federal Organizations

Ethics Codes and Standards for Licensed Clinicians

VA

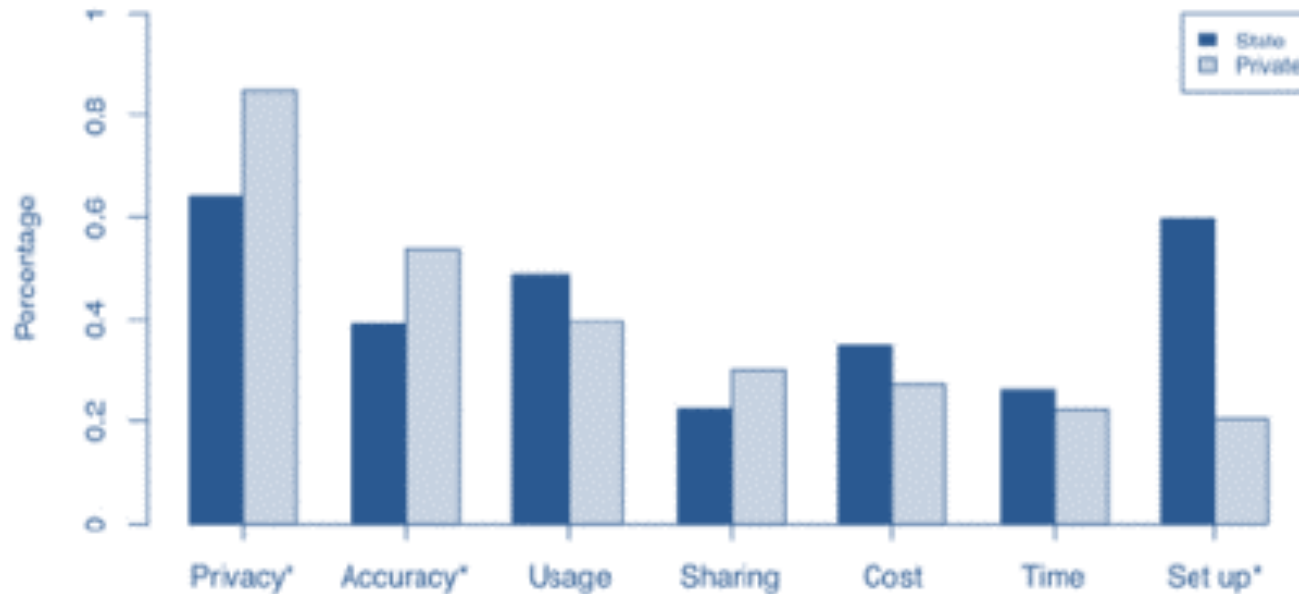


U.S. Department of Veterans Affairs  
Veterans Health Administration  
Office of Connected Care



# Security and Privacy Concerns are Barriers to Adoption of Mobile Health

- 32% “worried about security and privacy issues” (Physicians Practice, 2018)
- “Afraid of the potential security and privacy issues involved” was a common barrier cited by VA and DoD healthcare staff (Armstrong et al. 2018)
- Data privacy was top concern reported by patients regarding use of mobile health apps (Torous et al, 2018):





# What VA Staff Need to Know

## Core Competencies for Technology in Clinical Care



1. Evidence Base



2. Clinical  
Integration



3. Security and  
Privacy



4. Ethical Issues



5. Cultural  
Considerations



(Armstrong et al. 2018, Armstrong 2019)

**VA**



**U.S. Department of Veterans Affairs**

Veterans Health Administration  
Office of Connected Care



# VA Mobile Health Apps

VA U.S. Department of Veterans Affairs <https://mobile.va.gov/appstore>

VA Mobile ABOUT VA APP STORE NEWS & DISCUSSIONS DEVELOPERS FIELD TESTS PROGRAMS

## VA App Store

Here you will find access to dozens of apps, including those created specifically for Veterans and their Health Care Professionals.

All Apps Veterans Health Care Professionals

### FEATURED

| VA Online Scheduling                                   | VA Video Connect  | Exposure Ed   | VA Launchpad for Vete...                              |
|--|---|---|---|
| ★★★★★  | ★★★★★   | ★★★★★   | ★★★★★   |
| Schedule, request and track VA appointments with ease! | Secure video visits with your VA care team from anywhere. | Helpful resource for exposure-related health impacts. | One app to launch them all! Launch VA apps from here. |
| Web  | iOS Web Android   | iOS Android   | iOS Android   |

### TOP VETERAN APPS

See all >

| MOVE! Coach  | REVAMP App for Vetera...                                   | Stay Quit Coach  | VA Health Chat                             |
|--|--|--|--|
| ★★★★★  | ★★★★★  | ★★★★★  | ★★★★★                                      |
| Looking for weight loss support? This app is for that. | Pairs with your PRA? machine to track sleep apnea at home. | Create a tailored plan to help you quit and stay smoke-free. | Easy, online access to chat with VA staff. |
| iOS Android  | Web  | iOS Android  | Web  |



U.S. Department of Veterans Affairs  
Veterans Health Administration  
Office of Connected Care



# Types of VA Mobile Apps and Understanding the Differences

## VA Connected Apps



## VA Self-Contained Apps



**U.S. Department of Veterans Affairs**  
Veterans Health Administration  
Office of Connected Care





# VA Self-Contained Apps

## Data Security and Privacy:

- Private: Does not collect or require personal information
- Self-contained: Does not connect with VA's electronic health record
- Control: You own the data and can delete the app anytime



## Access and Content:

- Free & publicly available in the app marketplaces
- Section 508 compliant (accessible to those with disabilities)
- Evidence-informed content
- Tailored to Veterans & VA providers, but can be used by anyone
- In addition, all 'self-contained' apps:
  - Provide crisis resources
  - Allow progress-tracking
  - Provide health education & symptom management tools

Questions or comments: [MobileMentalHealth@va.gov](mailto:MobileMentalHealth@va.gov)



U.S. Department of Veterans Affairs  
Veterans Health Administration  
Office of Connected Care

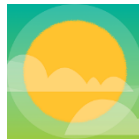
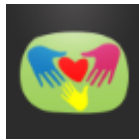
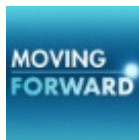




# VA Self-Contained Apps

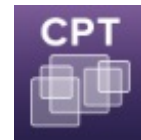
## Self-Care Apps

- **Self-management tools, that can be used by anyone, whether in treatment or not.**




## Treatment Companion Apps

**To be used in conjunction with evidence-based psychotherapies.**





A close-up photograph of an iPhone. The top of the device is visible, showing the earpiece, front-facing camera, and sensor. Below the status bar, the home screen is displayed with a dark space-themed wallpaper featuring stars. Three app icons are visible: a weather app with a yellow sun, the Camera app, and the Photos app. A white text box is overlaid on the right side of the image.

## Video: Demonstrating an App: Security and Privacy

<https://bcove.video/2TjsxB9>



8:49 PM



VA



U.S. Department of Veterans Affairs

Veterans Health Administration  
Office of Connected Care



# VA Connected Apps



## Data Security and Privacy:

- Secure: requires log in using an approved VA credential
- Private: VA personal health data is encrypted during transmission and when on VA secure network following strict federal standards of security and privacy
- Control: Connects with VA's network and allows patient to share data with health care team
- Apps for VA care teams are only available through VA's secure network. Other security controls help ensure protection meets strict federal standards of security and privacy.

## Access and Content:

- Access on <https://www.mobile.va.gov/appstore>
- Section 508 compliant (accessible to those with disabilities)



# VA Connected Apps for Health Care Professionals

- Communicates with the VA network
- Data is encrypted



## Airborne Hazards and...



Deployment-related exposures database for providers.

Web



## Annie App for Clinicians



Clinicians, meet Annie. She can help you support Veterans.

Web



## Image Viewing Solution



Now you see them! App to access diagnostic-grade images.

Web



## Patient Viewer



App to help efficiently find patient EHR data on the go.

Web



## REVAMP App for Clinici...



Tools to treat sleep apnea patients in their homes.

Web



## Scheduling Manager



For VA staff who manage online appointment requests.

Web



## Virtual Care Manager



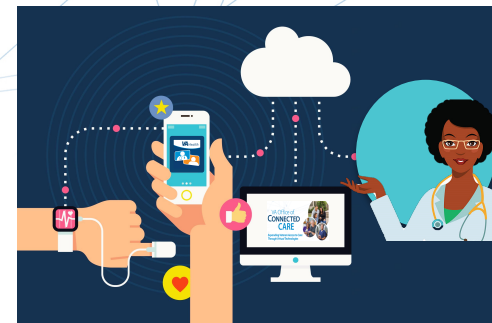
Create, view, and join video visits.

Web



# VA Connected Apps for Health Care Professionals

- Communicates with the VA network
- Data is encrypted



## Additional Resources:

- Requires authentication to log-in: via PIV, PIV exemption or Vista login credentials for VA staff
- PIV Linkage Guide:  
<https://mobile.va.gov/sites/default/files/piv-linkage-process.pdf>
- 2 minute tutorial on how to set up PIV-D  
<https://www.youtube.com/watch?v=DyA5YUBCCUQ&feature=youtu.be>





# VA Connected Apps for Veterans

- Communicates with the VA network
- Data is encrypted



## Airborne Hazards and...

Deployment-related exposures information for Veterans.

Web



## Annie App for Veterans

Meet Annie, she sends Veterans self-care messages.

Web



## Ask a Pharmacist

All your VA pharmacies and trusted medication info here.

Web



## MobileKidney

Track kidney health and learn about other disease topics.

Web



## Pain Coach App for Vet...

Pain Coach offers helpful tools to track and manage pain.

Web



## REVAMP App for Veter...

Pairs with your PAP machine to track sleep apnea at home.

Web



## VA Health Chat

Easy, online access to chat with VA staff.

iOS Web Android



## VA Online Scheduling

Schedule, request and track VA appointments with ease!

Web



## VA Video Connect

Secure video visits with your VA care team from anywhere.

iOS Web Android



## Rx Refill

Request, refill and track VA prescriptions with ease.

iOS Android



## Coming Soon: My VA Images



# VA Connected Apps for Veterans

- Communicates with the VA network
- Data is encrypted



## Additional Resources:

- Requires authentication to log-in (via My Health eVet Premium login, DS login, or ID.me)
- Find out more at:  
<https://www.myhealth.va.gov/mhv-portal-web/upgrading-your-my-healthevet-account-through-in-person-or-online-authentication>

A screenshot of the 'Department of Veterans Affairs Identity Provider Selection' screen. The screen has a dark blue header with the VA seal and the text 'Department of Veterans Affairs Identity Provider Selection'. Below the header, it says 'Please select how you would prefer to log in:'. There are three buttons: 'ID.me' with the text 'Use your ID.me account', 'DSLogon' with the text 'Use your DSLogon Level 2 account', and 'My Health eVet' with the text 'Use your My Health eVet Premium Account'.



# Being An Informed mHealth User





# A Trusted Source

**VA**



**U.S. Department of Veterans Affairs**  
Veterans Health Administration  
Office of Connected Care



# Permissions: What Are They?

- Some apps are designed to leverage specific hardware or software capabilities on your device.
- Common permissions include access to your device's:
  - Calendar
  - Camera
  - Contacts
  - Photos
  - Music





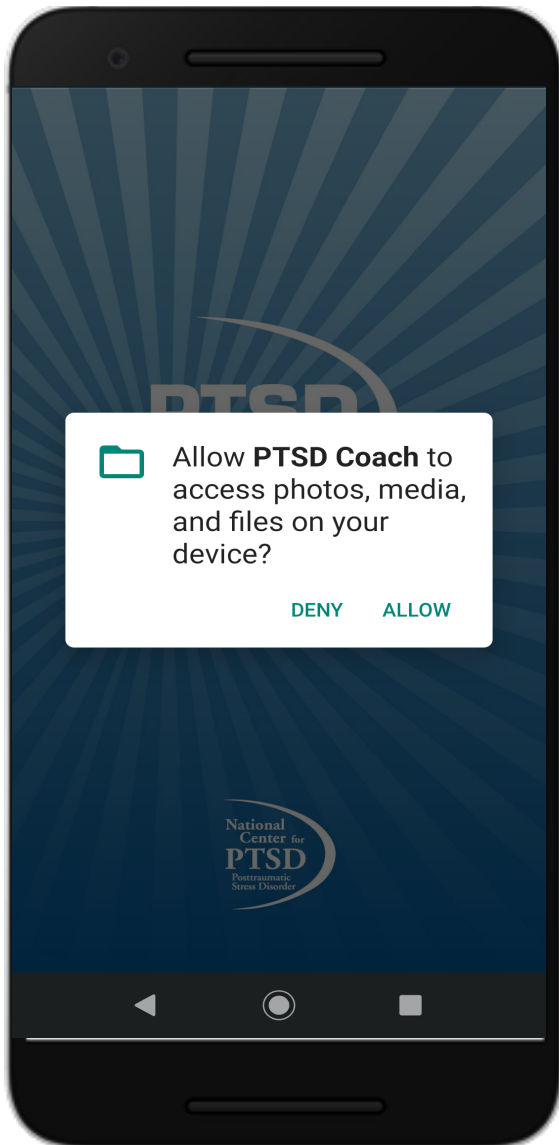
# Permissions: Knowing When To Grant Them

**Before** you grant permissions in an app, you should make sure that:

- The developer has clearly explained why they need these permissions
- You understand the request and it makes sense with respect to the purpose of the app

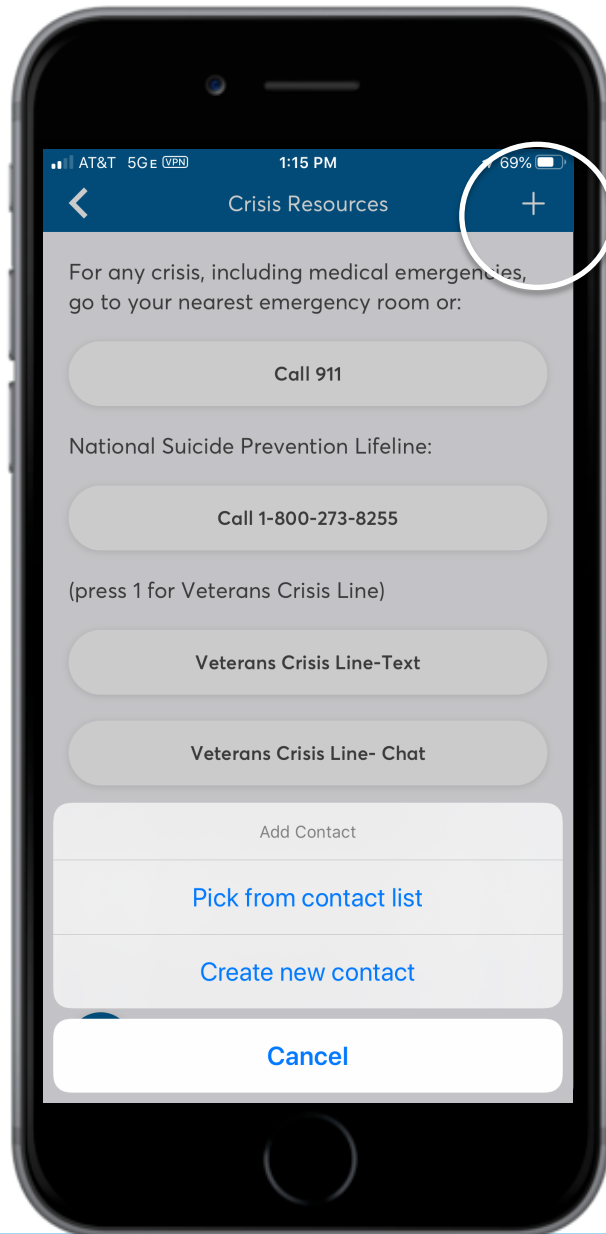


# Android Permissions Example: PTSD Coach



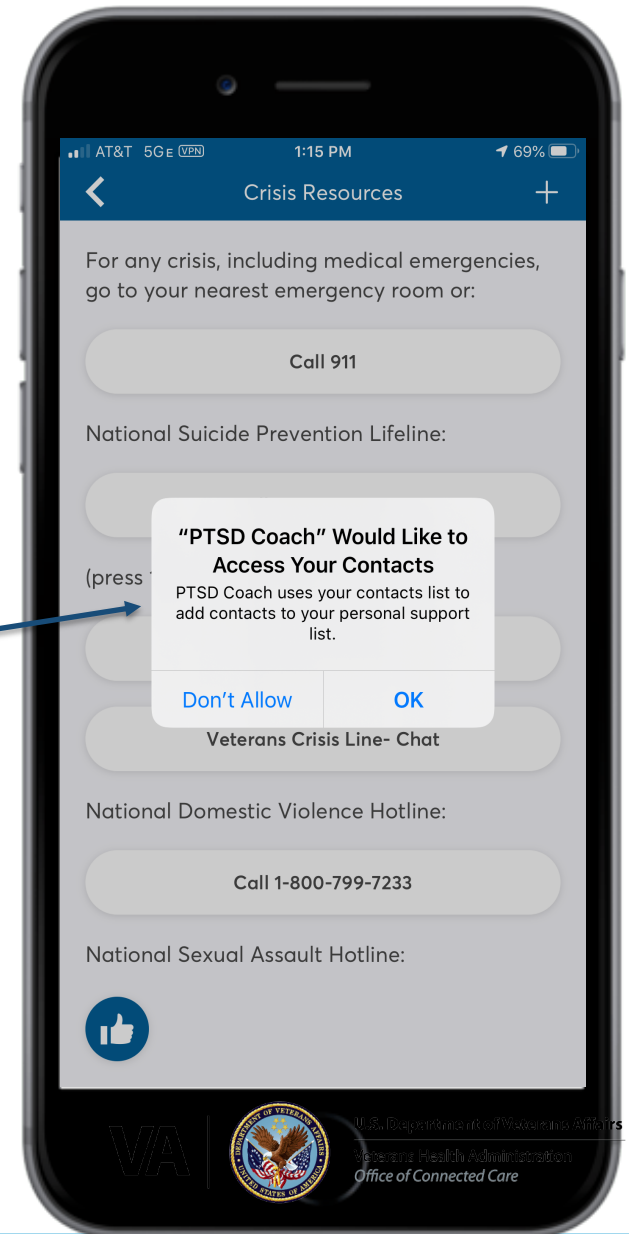


# iOS Permissions Example: Access Your Contacts



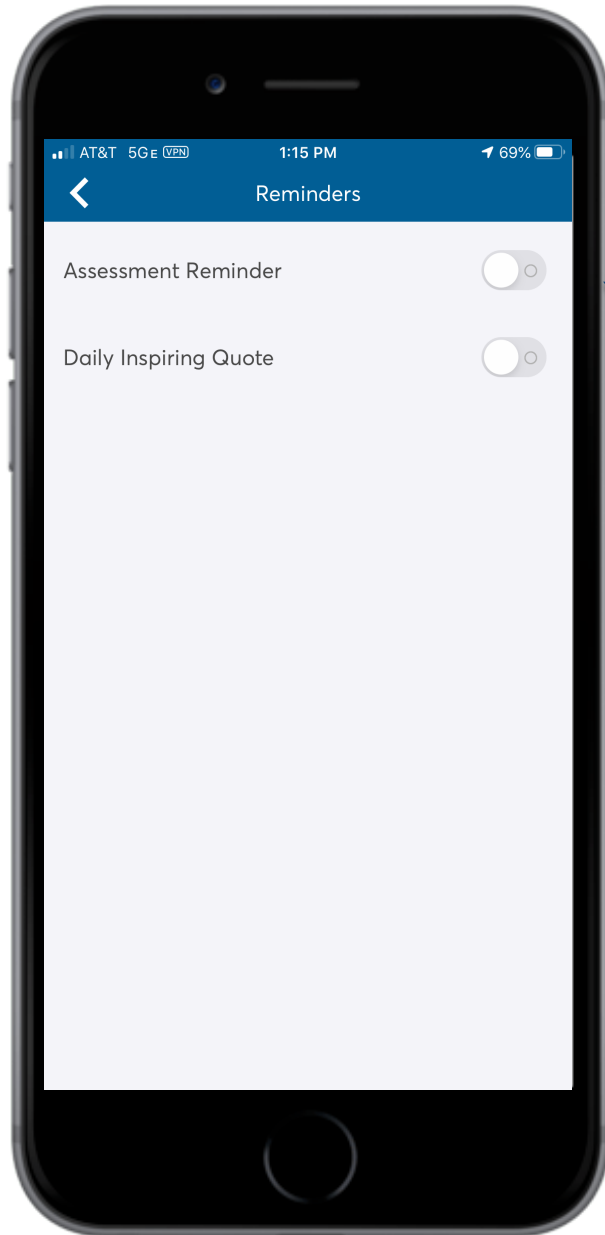
Action you want to take in the app  
(Add contact)

How the app allows you to add contact to app

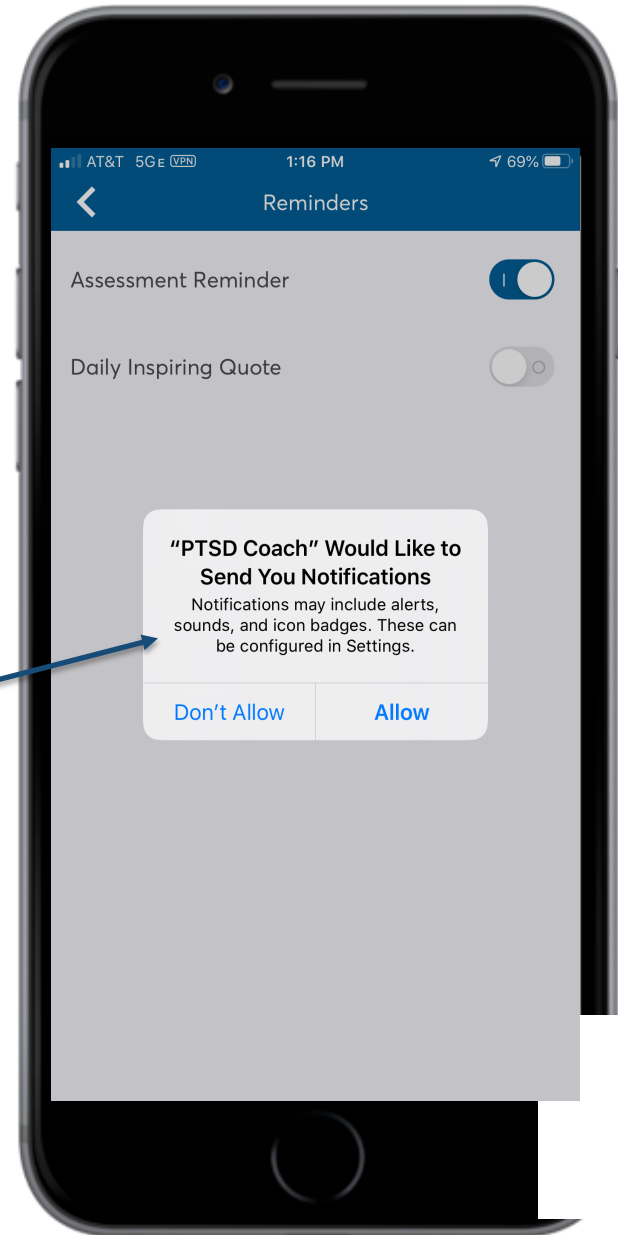




# iOS Permissions Example: Send Notifications



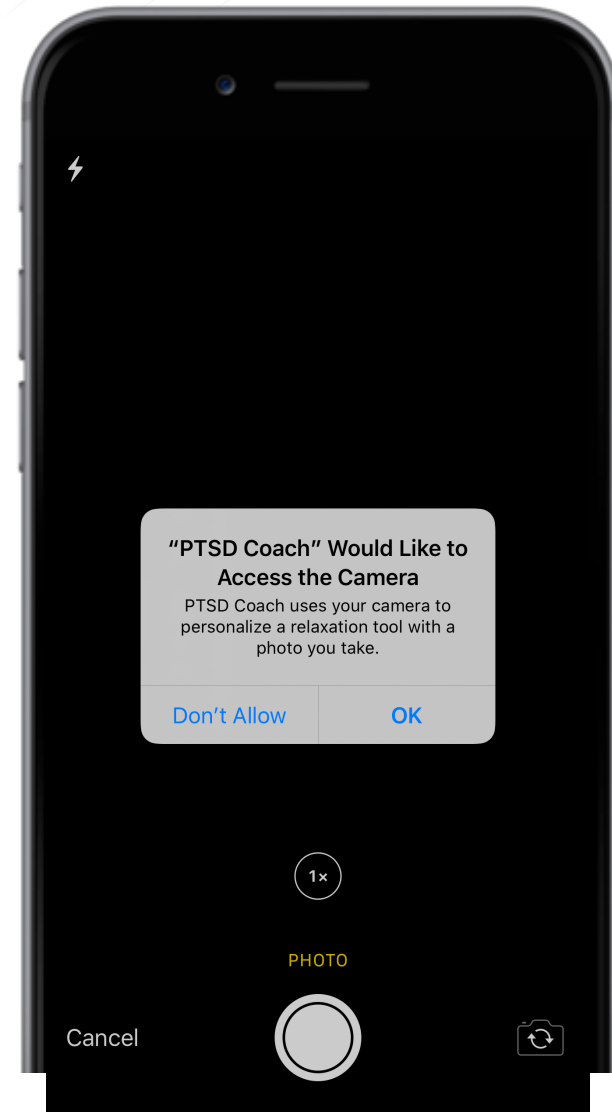
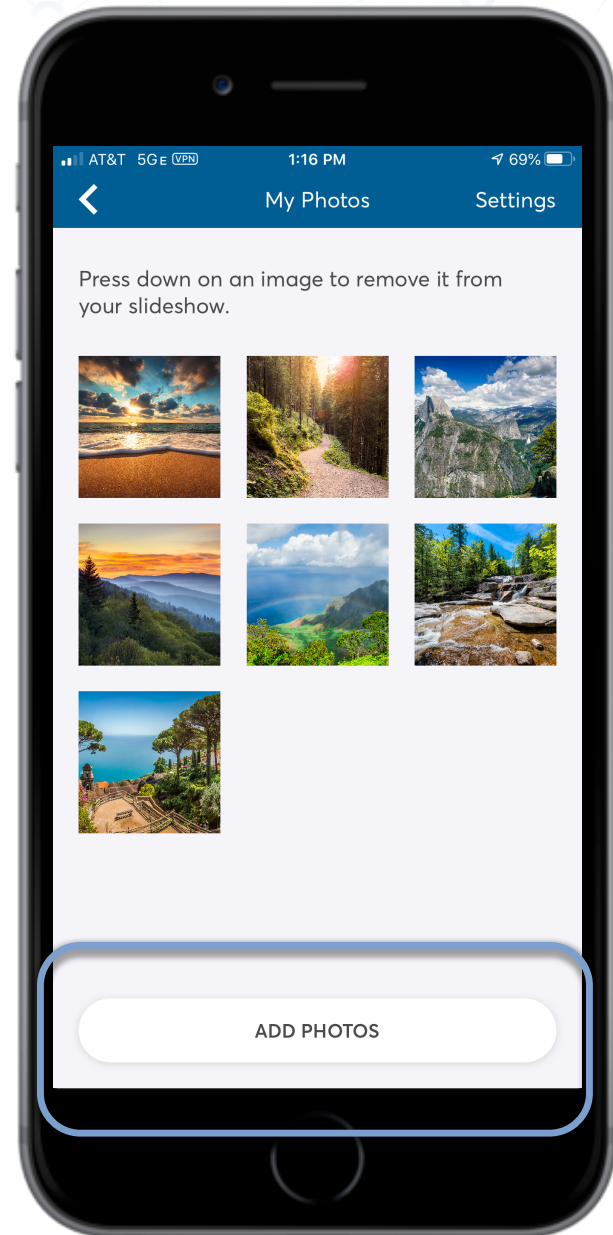
Action you want  
to take in the app  
(Add reminders)



How the app  
allows you to add  
reminders

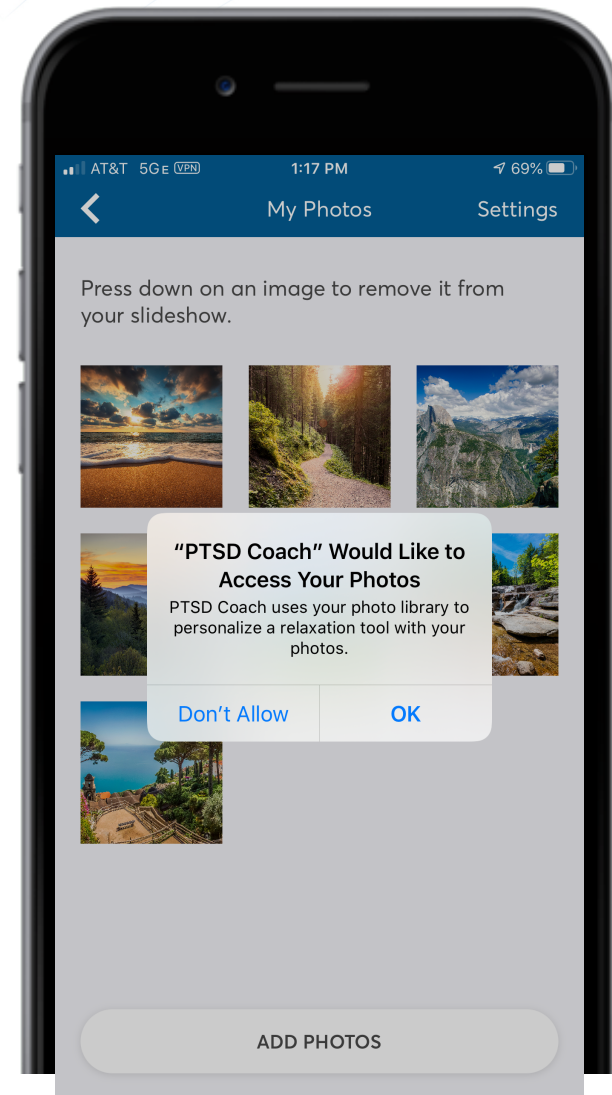
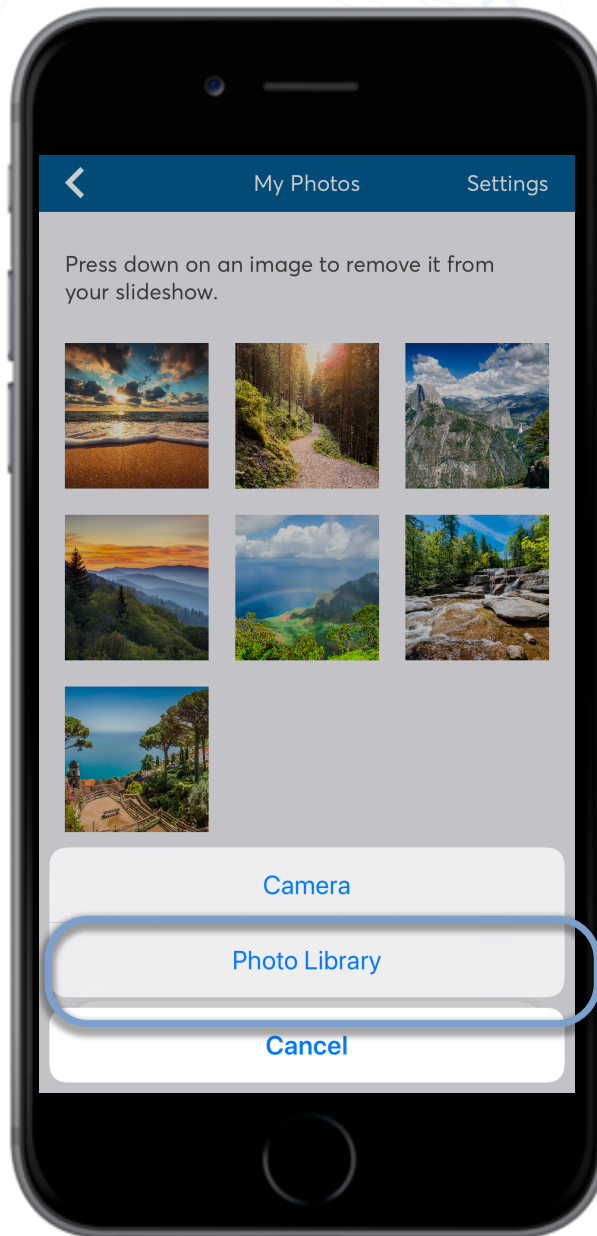
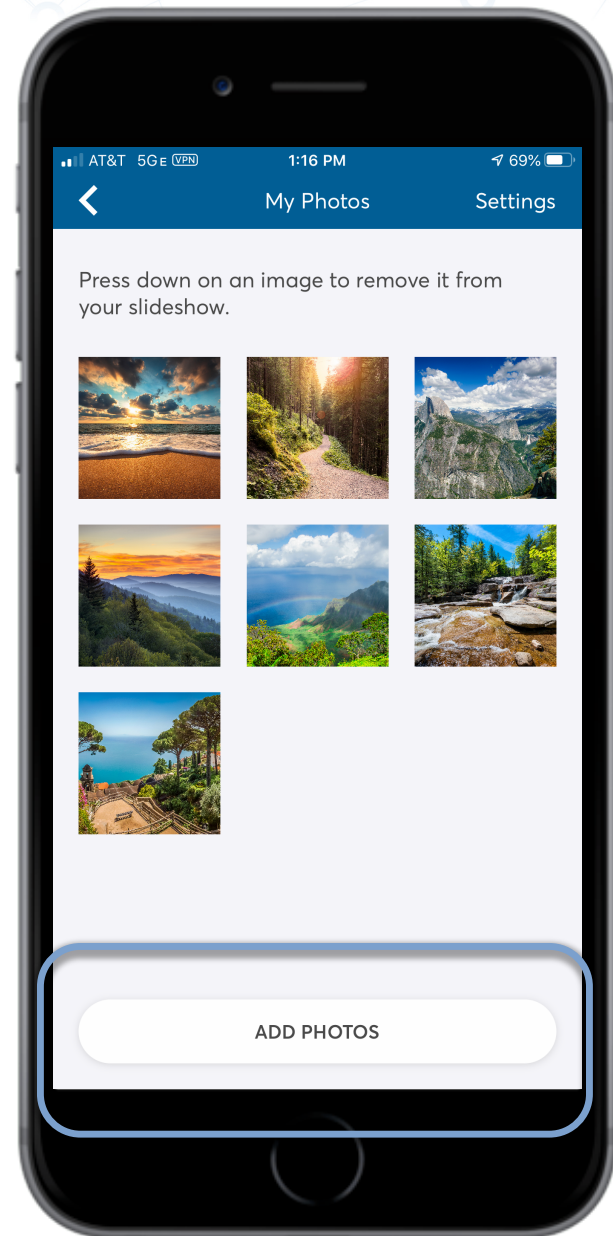


# iOS Permissions Example: Access Your Camera



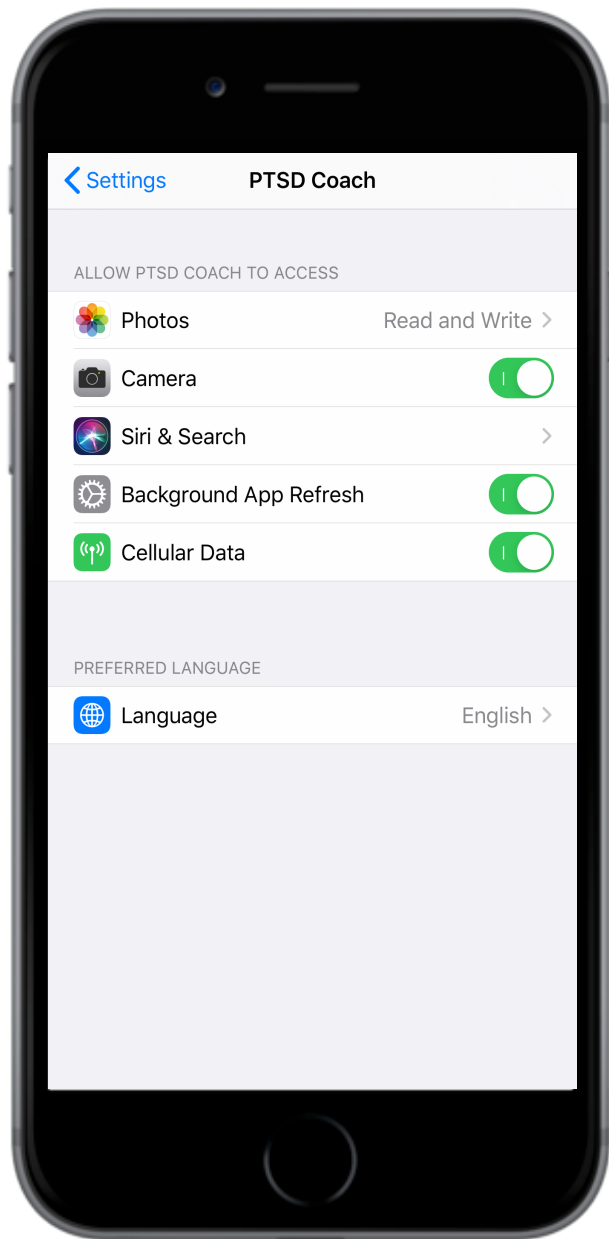


# iOS Permissions Example: Access Photos





# iOS Permissions Example: Reviewing Settings





# Where are these data stored?

For VA self-contained apps:

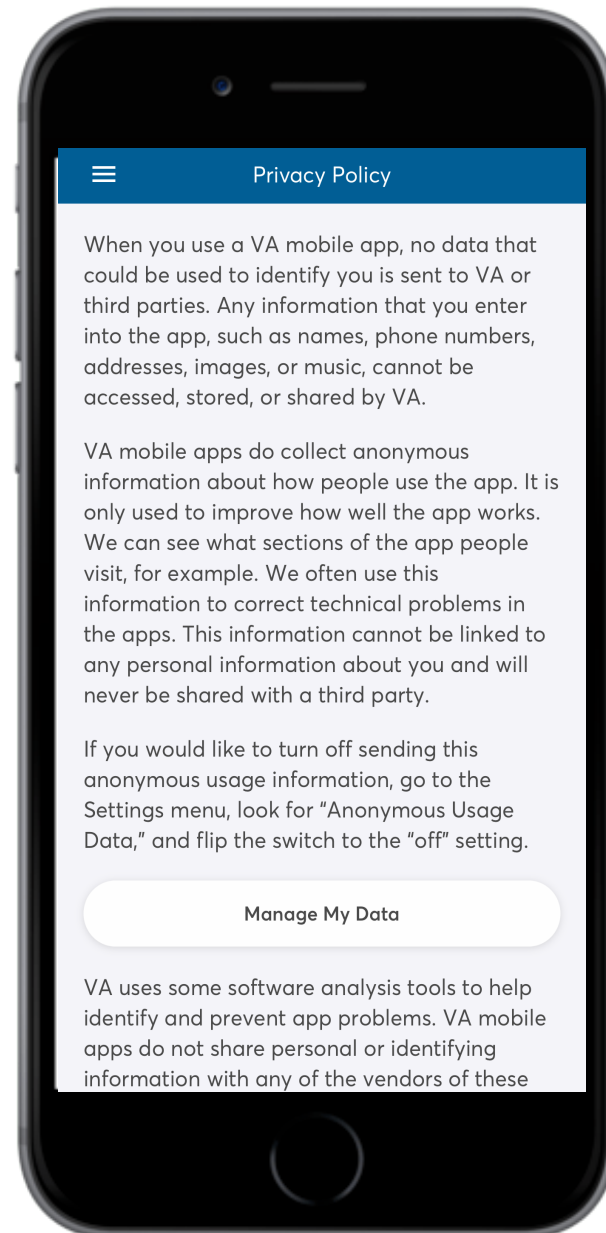
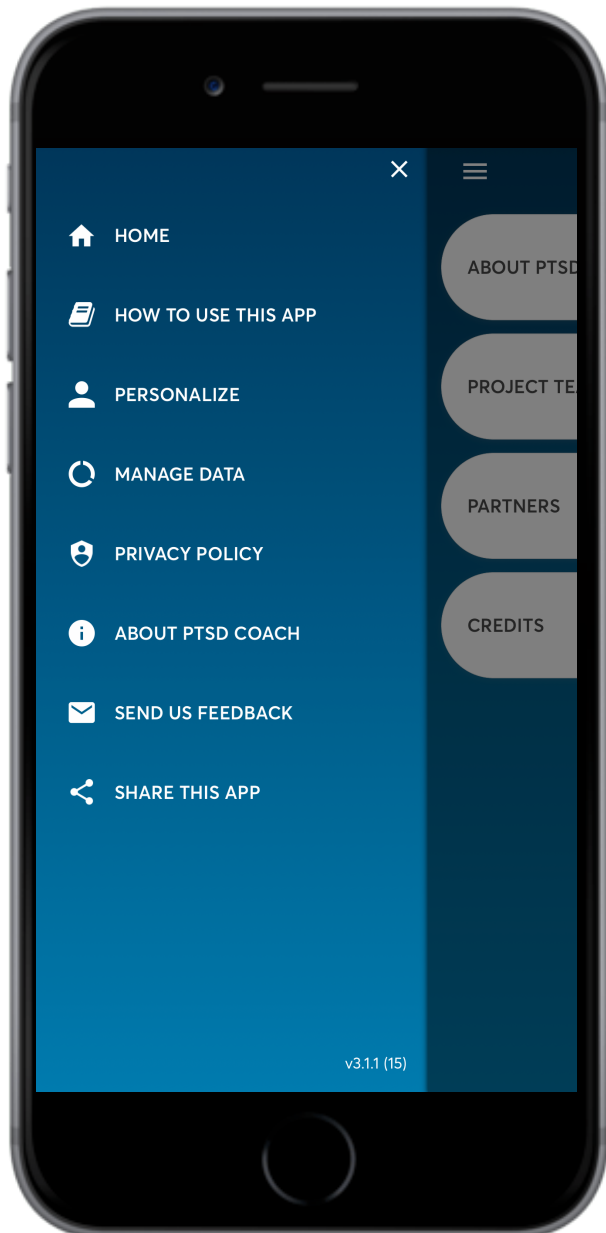
Data are stored only on the mobile device

Personally identifying data are not shared with the VA or any third-party vendors.

If users have enabled cloud backup for some/all apps, app data are backed up and sent to backup servers (e.g., iCloud for iOS)



# For More Information: Privacy Policies





# Key Questions to Consider When Evaluating mHealth apps

- Who made the app?
- What data are collected?
- Where are data stored?
- Who has access to the data? How can the data be used?
- What are the alternative options to using a virtual care tool?





# Good Privacy and Security Practices with Mobile Health



# Mobile Health Security and Privacy Handout for Patients and Providers

Provides key information to patients and providers on the protection of mobile health data

Can be used as a resource to frame discussions providers may have with patients interested in mobile health security

## How Can You Protect and Secure Health Information When Using a Mobile Device?



### 1. Use a password or other user authentication

Authentication is the process of verifying the identity of a user, process, or device. Mobile devices can be configured to require passwords, personal identification numbers (PINs), or passcodes to gain access to it. The password, PIN, or passcode field can be masked to prevent people from seeing it. Mobile devices can also activate their screen locking after a set period of device inactivity to prevent an unauthorized user from accessing it.



### 2. Install and enable encryption

Encryption protects health information stored on and sent by mobile devices. Mobile devices can have built-in encryption capabilities, or you can buy and install an encryption tool on your device.



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

**Remote wiping** enables you to erase data on a mobile device remotely. If you enable the remote wipe feature, you can permanently delete data stored on a lost or stolen mobile device.

**Remote disabling** enables you to lock or completely erase data stored on a mobile device if it is lost or stolen. If the mobile device is recovered, you can unlock it.



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

File sharing is software or a system that allows Internet users to connect to each other and trade computer files. But file sharing can also enable unauthorized users to access your laptop without your knowledge. By disabling or not using file sharing applications, you reduce a known risk to data on your mobile device.



### 5. Install and enable a firewall

A personal firewall on a mobile device can protect against unauthorized connections. Firewalls intercept incoming and outgoing connection attempts and block or permit them based on a set of rules.



### 6. Install and enable security software

Security software can be installed to protect against malicious applications, viruses, spyware, and malware-based attacks.



### 7. Keep your security software up to date

When you regularly update your security software, you have the latest tools to prevent unauthorized access to health information on or through your mobile device.



### 8. Research mobile applications (apps) before downloading

A mobile app is a software program that performs one or more specific functions. Before you download and install an app on your mobile device, verify that the app will perform only functions you approve of. Use known websites or other trusted sources that you know will give reputable reviews of the app.



### 9. Maintain physical control

The benefits of mobile devices - portability, small size, and convenience - are also their challenges for protecting and securing health information. Mobile devices are easily lost or stolen. There is also a risk of unauthorized use and disclosure of patient health information. You can limit an unauthorized users' access, tampering or theft of your mobile device when you physically secure the device.



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

Public Wi-Fi networks can be an easy way for unauthorized users to intercept information. You can protect and secure health information by not sending or receiving it when connected to a public Wi-Fi network, unless you use secure, encrypted connections.



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

When you use software tools that thoroughly delete (or wipe) data stored on a mobile device before discarding or reusing the device, you can protect and secure health information from unauthorized access. HHS OCR has issued guidance that discusses the proper steps to take to remove health information and other sensitive data stored on your mobile device before you dispose or reuse the device.

Source: <http://www.healthit.gov/providers-professionals/how-can-you-protect-and-secure-health-information-when-using-mobile-device>

NOTE: The content on the Mobile Device Privacy and Security subsection of HealthIT.gov is provided for informational purposes only and does not guarantee compliance with Federal or state laws. Please note that the information and tips presented may not be applicable or appropriate for all health care providers and professionals. We encourage providers, professionals, and organizations to seek expert advice when evaluating these tips. The Mobile Device Privacy and Security subsection of HealthIT.gov is not intended to be an exhaustive or definitive source on safeguarding health information from privacy and security risks. It is also not intended to serve as legal advice or offer recommendations based on a provider's or professional's specific circumstances. For more information about the HIPAA Privacy and Security Rules, please visit the HHS Office for Civil Rights Health Information Privacy website.



# Password Protection



Phone  
App

**VA**



**U.S. Department of Veterans Affairs**

Veterans Health Administration  
Office of Connected Care



# Maintain Control

Install Remote Wiping and/or  
Remote Disabling



**U.S. Department of Veterans Affairs**

Veterans Health Administration  
*Office of Connected Care*





# Public Wi-Fi

When you're on the same network it's possible to steal someone's username and password or see what they're doing...

- Turn off sharing
- Enable your firewall
- When in doubt, put phone in airplane mode
- Turn Wi-Fi off when not using it



# Security and Privacy Resources

## **VA Mobile Health Provider Program**

<https://mobile.va.gov/providers/training>

## **U.S. Department of Health and Human Services – Mobile Devices**

<https://www.hhs.gov>

## **Health IT.gov Mobile Device Privacy and Security**

<https://Healthit.gov/mobiledevices>

<https://www.healthit.gov/video/mobile-health-security-important>

## **Overview of Federal Role in Mobile Health**

<https://www.healthit.gov/resource/your-mobile-device-and-health-information-privacy-and-security>

## **Mobile devices roundtable: safeguarding health information**

<https://www.healthit.gov/policy-researchers-implementers/mobile-devices-roundtable-safeguarding-health-information>

## **HIPAA Laws and Regulations Overview**

<https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>



# Video Series on Mobile Health Security

<https://www.healthit.gov/video/mobile-health-security-important>



Official Website of The Office of the National Coordinator for Health Information Technology (ONC)

Connect with us:



TOPICS | HOW DO I? | BLOG | NEWS | ABOUT ONC

Search



Home

## Topics

How Do I?

For Providers



For Developers & Vendors



For Individuals

Blog

News

Events



Fact Sheets

Infographics

Multimedia

New Funding Announcements

News Releases



Recent Updates

About ONC

Health IT Feedback Form

Health IT Strategic Planning

## Mobile Health Security is Important!



Dec 12, 2012 | 4:08

Mobile health security is no joke. It is important to protect the security of your mobile health devices. Learn more about why it is important for providers to pay attention and to address the privacy and security of patient's electronic health information when using mobile health devices.

Visit the mobile health device privacy and security website to learn more about practical ways to protect and secure patient's health information when using mobile health devices:

<http://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security>.

## Watch Other Videos





# Key Takeaways

- You have a responsibility to understand and discuss issues relating to security and privacy with patients
- For apps that don't require user authentication, VA only has access to aggregated data
- For VA apps that connect to the health record, the VA does have access to this data, but it is protected by privacy laws and regulations

VA



U.S. Department of Veterans Affairs

Veterans Health Administration

© 2015 by U.S. Department of Veterans Affairs



# VA Mobile Resources and Training



## VA Mobile Health

<https://www.mobile.va.gov/appstore>

<https://mobile.va.gov/appstore/all>

## VA Mobile Mental Health App Resources

Tech into Care SharePoint site: <https://tinyurl.com/Tech-Into-Care>

Practice-Based Implementation (PBI) Network CE Lecture Series:  
[www.myvaapps.com/pbi-network-ce-lecture-series/](http://www.myvaapps.com/pbi-network-ce-lecture-series/)

App overviews, demo videos, and download links: [www.ptsd.va.gov/appvid/mobile](http://www.ptsd.va.gov/appvid/mobile)



## VA Annie

Clinician Training:

Every Wednesday at 1:00pm EST between now and May 20th. (email to be put on distribution list: [VACOAnnieRT@va.gov](mailto:VACOAnnieRT@va.gov))

Annie SharePoint site:

[https://vaww.connectedhealth.va.gov/mhd/VAMR/Annie/\\_layouts/15/start.aspx](https://vaww.connectedhealth.va.gov/mhd/VAMR/Annie/_layouts/15/start.aspx)

Annie app for Clinicians: <https://mobile.va.gov/app/annie-app-clinicians>



# VA Connected Care Resources and Training

## *Office of* **CONNECTED CARE**



### **Office of Connected Care**

Communication Toolkits:

<https://vaww.connectedhealth.va.gov/Communications/SitePages/homepage.aspx>

### **VA Connected Care Discussion Series**

Monthly webinar series: <https://mobile.va.gov/discussion-series>

### **VA Connected Care Integrated Care Series**

Webinar series on integrating virtual care tools:

(email to be put on distribution list: [Sherron.Olliff@va.gov](mailto:Sherron.Olliff@va.gov))

### **VA Connected Care Community of Practice**

(email to be put on distribution list: [Chimplementation@va.gov](mailto:Chimplementation@va.gov))

### **VA Telehealth Services**

<https://www.telehealth.va.gov>

Telehealth Document Library:

<https://vaww.infoshare.va.gov/sites/telehealth/docs/Forms/AllItems.aspx>

### **My HealtheVet**

<https://myhealth.va.gov>

Intranet: <http://vaww.va.gov/MYHEALTHEVET/>

Marketing and Promotion Toolkit:

[http://vaww.va.gov/MYHEALTHEVET/promotion\\_communication.asp](http://vaww.va.gov/MYHEALTHEVET/promotion_communication.asp)



**U.S. Department of Veterans Affairs**

Veterans Health Administration  
Office of Connected Care



# Who do I call for help?



## **VA Mobile Solutions Help Desk**

Veterans - 1-877-470-5947

VA care team - 1-844-482-6624

Monday to Friday: 7 a.m. – 7 p.m. CT

For technical questions, bugs, or suggestions for the “self-contained” or mobile mental health apps [MobileMentalHealth@va.gov](mailto:MobileMentalHealth@va.gov)



## **National Telehealth Technology Help Desk**

866-651-3180

Monday to Saturday: 7 a.m. - 10 p.m. CT



## **My HealtheVet Help Desk**

877-327-0022

Monday to Friday: 7 a.m. – 7 p.m. CT



**Questions?**





# Thank you!

VA Office of Connected Care  
[www.connectedcare.va.gov](http://www.connectedcare.va.gov)

VA National Center for PTSD  
[www.ptsd.va.gov](http://www.ptsd.va.gov)

*Office of*  
**CONNECTED  
CARE**

National Center for  
**PTSD**  
POSTTRAUMATIC STRESS DISORDER



# References

- Armstrong, C. M. (2019). Mobile health provider training: Results and lessons learned from year four of training on core competencies for mobile health in clinical care. *Journal of Technology in Behavioral Sciences*. doi:10.1007/s41347-019-00089-8, online preprint sharing <https://rdcu.be/btchQ>
- Armstrong, C. M., Ciulla, R. P., Edwards-Stewart, A., Hoyt, T., & Bush, N. (2018). Best practices of mobile health in clinical care: the development and evaluation of a competency-based provider training program. *Professional Psychology: Research and Practice*, 49(5-6), 355-363. [doi:10.1037/pro0000194](https://doi.org/10.1037/pro0000194)
- Armstrong, C. M., Edwards-Stewart, A., Ciulla, R. P., Bush, N. E., Cooper, D. C., Kinn, J. T., Pruitt, L. D., Skopp, N. A., Blasko, K. A., & Hoyt, T. V. (2018). *Department of Defense Mobile Health Practice Guide, fourth edition*. Connected Health Branch, Defense Health Agency, U.S. Department of Defense. [https://www.researchgate.net/publication/326842558\\_DoD\\_Mobile\\_Health\\_Practice\\_Guide\\_4th\\_Edition](https://www.researchgate.net/publication/326842558_DoD_Mobile_Health_Practice_Guide_4th_Edition)
- Edwards-Stewart, A., Alexander, C., Armstrong, C. M., Hoyt, T., & O' Donohue, W. (2018). Mobile applications for client use: Ethical and legal considerations. *Psychological Services*, 15. [doi:10.1037/ser0000321](https://doi.org/10.1037/ser0000321)
- Food and Drug Administration (2015). Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff. <https://www.fda.gov/media/80958/download>  
<https://www.fda.gov/medical-devices/digital-health/mobile-medical-applications>
- Harris, E., & Younggren, J. N. (2011). Risk management in the digital world. *Professional Psychology: Research and Practice*, 42(6), 412-418. doi:10.1037/a0025139
- Health IT.gov Mobile Device Privacy and Security <https://Healthit.gov/mobiledevices>
- Hoffman L, Benedetto E, Huang H, Grossman E, KalumaKalumaD, Mann Z, Torous J. Augmenting D, Mann Z, Torous J. Augmenting Mental Health in Primary Care: Mental Health in Primary Care: A One--Year Study of Deploying Smartphone Apps in a MultiYear Study of Deploying Smartphone Apps in a Multi--Site Primary Care/Behavioral Health Integration Program. *Frontiers in psychiatry*. 2019;10:94.Site Primary Care/Behavioral Health Integration Program. *Frontiers in psychiatry*. 2019;10:94.
- Jones, N., & Moffitt, M. (2016). Ethical guidelines for mobile app development within health and mental health fields. *Professional Psychology: Research and Practice*, 47(2), 155-162. doi:10.1037/pro0000069
- Karcher, N. R., & Presser, N. R. (2016). Ethical and Legal Issues Addressing the Use of Mobile Health (mHealth) as an Adjunct to Psychotherapy. *Ethics & Behavior*, 1-22. doi:10.1080/10508422.2016.1229187
- Mobile devices roundtable: safeguarding health information <https://www.healthit.gov/policy-researchers-implementers/mobile-devices-roundtable-safeguarding-health-information>  
<https://ec.europa.eu/digital-single-market/en/news/current-initiatives-unlock-potential-mobile-health-europe>
- Overview of Federal Role in Mobile health <https://www.healthit.gov/policy-researchers-implementers/overview-federal-role-mobile-health>
- Torous J, Wisniewski H, Liu G, KeshavanKeshavanM. Mental Health M. Mental Health Mobile Phone App Usage, Mobile Phone App Usage, Concerns, and Benefits Among Concerns, and Benefits Among Psychiatric Outpatients: Psychiatric Outpatients: Comparative Survey Study. *JMIR Comparative Survey Study. JMIR Mental Health. Mental Health*. 2018;5(4):e117152018;5(4):e11715
- Torous, J. (2019) Informed and Shared Decision Making around Smartphone Apps for Clinical Care.
- U.S. Department of Health and Human Services – Mobile Devices <https://www.hhs.gov>
- VA Mobile Health Provider Program <https://mobile.va.gov/providers/training>