



GETTING HELP

If you need help at any time, you can reach the UF Health IT team using one of these methods:

- **Over the phone**
Gainesville: (352) 265-0526
Jacksonville: (904) 244-7828
24 hours a day, every day
- **In Person, in Gainesville**
Communicore C2-011
8am-5pm, Monday - Friday
- **Online service request**
ithelp.ahc.ufl.edu
- **Online information**
bridge.ufhealth.org/it
- **Self-help**
bridge.ufhealth.org/it-knowledge

REPORTING URGENT ISSUES

Please remember that **URGENT** issues must be submitted by calling first.

IN THIS HANDOUT

- [GETTING HELP](#)
- [GETTING YOUR COMPUTER READY](#)
- [ACCESS & ACCOUNTS](#)
- [CONNECT TO WIRELESS](#)
- [CONNECT TO VPN](#)
- [CONNECT TO EMAIL](#)
- [ADVANCED EMAIL](#)
- [UF HEALTH CITRIX & EPIC](#)
- [STORING & SHARING YOUR FILES](#)
- [COLLEGE APPLICATIONS](#)
- [INFORMATION SECURITY](#)
- [ADDITIONAL RESOURCES](#)
- [SPOK ON-CALL SYSTEM](#)
- [USING YOUR DESK PHONE](#)
- [LAPTOP PROTECTION VERIFICATION FORM](#)

UF Health Bridge

Bridge is an internal portal for all UF Health staff, faculty, and students that facilitates collaboration and communication. Many links & resources are available by visiting: <https://bridge.ufhealth.org>



GET YOUR COMPUTER READY

Take advantage of the computing resources that are available to you and ensure that your computer is secure and ready to go.

Microsoft Office 365

UF offers you free Office 365 which includes: Word, Excel, PowerPoint, OneNote, Access, Publisher, Outlook, and Skype for Business, and OneDrive for Business.

Get Office 365 from here:

<https://it.ufl.edu/services/gatorcloud-microsoft-office-online>

1. Click Go To Service.
2. Type your UF email address and the site will redirect you. Then login with your GatorLink account.
3. Once logged in choose the Install button.

Internet Browsers

Most resources you use will work in most browsers. However, if you run into issues it is a good idea to try Internet Explorer for Windows or Safari for Macs

UF OnTheHub

You might be eligible for free or discounted software. Visit UF OnTheHub at <https://portal.helpdesk.ufl.edu/>

Windows 10 for Education

Some computers come with Windows 10 Home. Some resources might not be available to you in this restricted version. However, UF offers you Windows 10 for Education. This is provided free of charge to you. Visit: <https://portal.helpdesk.ufl.edu/>

COMPUTER SECURITY

Your computer must be configured to comply with UF mobile device security policies. To comply, you will need to ensure that Antivirus is installed, Firewall is enabled, Disk encryption is enabled, and Automatic Updates are on.

Configure Windows

Antivirus/Firewall

Microsoft's Windows Defender is available to you for free and is built in to Windows 10. Ensure that Virus & Firewall protection is enabled by typing Windows Defender from your start menu and opening Windows Defender Security Center.

Encryption

Microsoft BitLocker is available for free in windows 10 Pro, Enterprise and Education versions. To enable BitLocker type BitLocker into the Start menu and open Manage Bitlocker. Choose Turn on Bitlocker then carefully follow the setup prompts. **Note:** If you do not have BitLocker settings, consider upgrading to Windows 10 for Education (refer to the information in this guide about Windows 10 for Education)

Automatic Updates

Type Updates in the Start menu then choose "Check for Updates". Ensure that your windows is up to date and that updates will automatically download.

Configure MacOS

Antivirus

MacOS does not have Antivirus installed by default. So you will need to install 3rd Party antivirus software. Some recommended free solutions are available to you

- Avast anti-virus: <https://www.avast.com/>
- AVG anti-virus: <http://www.avg.com/>

Encryption/Firewall

FileVault II is already available in MacOS. To enable FileVault, go to System Preferences > Security & Privacy > FileVault tab. Click the Lock to make changes then choose Turn on File Vault. While here, choose the Firewall tab and click Turn on Firewall.

Automatic Updates

Go to System Preferences > App Store. Then check mark the automatically check for updates



ACCESS & ACCOUNTS

Access to UF Health systems

Your program administrator has likely already secured access for you. However, if you are missing something your administrator must submit an access request form for any new access or changes to existing access by using IT service request system at <http://ithelp.ahc.ufl.edu>

ABOUT ACCESS REQUESTS

In most situations, your program administrator will need to request access on your behalf.

New access requests or modifications can take 3-5 business days to complete.

Update your contact information

For UF:

You can update your contact information through myUFL.

1. Visit my.ufl.edu
2. Choose the “Access myUFL” button
3. Login with your GatorLink account
4. Go to Main Menu
 - Hover over My Account
 - Choose My Directory Profile
5. Update your contact information

Manage your user account

For your GatorLink account:

1. Visit account.it.ufl.edu
2. Choose the best option for your needs
3. Follow the prompts to complete your actions

If for some reason you do not have a GatorLink account, please call the IT Support Center at 265-0526

For your Shands account:

You may have received a Shands user account to access various clinical applications.

Visit myaccount.shands.ufl.edu

- You will need to register for this site first
- Once registered you can manage your account

1. Choose the best option for your needs
2. Follow the prompts to complete your actions



CONNECT TO UF WIRELESS

The UF wireless network is available in all UF Health buildings. All UF Health faculty, staff, and students with a valid GatorLink or Shands user account can use this network.

Connect using Android or iOS mobile devices

1. Ensure that your Wireless is on and not in Airplane mode
2. From your wireless network list, select and connect to the “**UF**” wireless network
 - If using Android, make these settings:
EAP Method: PEAP
Phase 2 authentication: MSCHAPV2
3. Enter user account:
 - **UF:** enter your GatorLink username in the User or Identity field
4. Enter your password in the Password field
5. Choose Next, Connect or Done
6. If prompted, choose the ‘trust’ button to accept the security certificate

You should now be connected to the UF wireless network and the wireless indicator icon should display in your devices’ notifications area.

BEFORE YOU GET STARTED

For UF security compliance, you will need to have the latest version of Java from java.com, anti-virus software, have the latest operating system’s security updates installed, and your firewall enabled.

You will need install CloudPath on your computer before you can access UF Wireless.

Connect using Windows or Mac computers

1. Find your “Network Connections” icon in the toolbar near your system clock. Click the icon to view the available wireless networks
2. From the list of wireless networks, choose to connect to UFINFO
3. Ensure the connection dialog indicates, “Connected.”
4. Open your web browser and it should automatically connect you to getonline.ufl.edu. If not, manually browse to getonline.ufl.edu
5. Click “Auto Configuration”
6. Download and run the CloudPath client for your particular operating system.
7. Follow the prompts to configure Cloudpath.
8. During the CloudPath client install, you may see Warnings that prompt you for administrative privileges to make settings changes to your computer. Please allow or accept any request for settings change

When finished, this installer should automatically change your connection to the listed “UF” wireless network. If it does not, please try to reconnect to UF wireless manually.

In some cases you may need to “Forget” the UF and UFINO wireless networks then try to manually connect back to UF wireless.

Forgetting/Remove Wireless Network Profiles

Sometimes you might need to forget/remove the UF wireless network from your device then reconnect.

iOS or Android

- 1) Open settings then find your wireless network list.
- 2) Tap the UF wireless profile then locate the option to forget or remove the UF wireless profile.

Mac

- 1) Open Network Preferences from your wireless menu.
- 2) Choose Advanced then find and click the UF wireless profile in the list then click the minus button.

Windows 10

- 1) Open Network & Internet Settings from your wireless menu.
- 2) On the left, Choose Wi-Fi then choose Manage known networks.
- 3) Find and click the UF wireless profile then choose “Remove”.



CONNECT TO VPN

UF Health VPN is supported on all modern computers and mobile operating systems

VPN Web Portal

1. In the address field of your web browser, type in “vpn.ufhealth.org” and press enter
2. This takes you to the UF Health VPN Web Portal
3. Choose your Realm and enter your login information. Then choose “Sign In”
4. Pick from any Web Bookmarks and other resources located on the VPN Portal

VPN WEB PORTAL

You may see Setup notifications that prompt you for administrative privileges to make changes to your computer. Please always **allow** or **accept** any request for settings change.

If this is your **FIRST** time connecting to the VPN web portal, you might see a request to restart your computer.

Desktop VPN Client

A client (Pulse Secure) is available to connect to VPN from your Windows or Mac computer. VPN will allow you to access UF Health systems as if you were onsite.

1. Visit ufhealth.org/vpn
2. Choose and download the client to install from the right hand side
3. From this download, install the Pulse Secure Client per the onscreen prompts
4. Click the **UF Health** connection
5. When prompted, choose the appropriate realm
6. Enter your login information
7. Choose **Sign In**

When connected properly, you will see the **connected**

Pulse Secure VPN client icon in the application tray near the system clock.

Mobile VPN

1. Ensure that you have a wireless or data connection
2. Go to your “App Store”
3. Search for and install Pulse Secure
4. Once installed, open the Pulse Secure app
5. At the app’s configuration screen, add a new connection with the following settings:

Connection name: UF Health

Server name: vpn.ufhealth.org

Username: yourusername

Password: youraccountpassword

Realm/Domain: UFAD

6. Tap on the newly listed connection item to connect

MOBILE VPN

When connection is properly set, you will see the VPN connection indicator in the notifications area on your device.

If you want to disconnect from VPN, you must reopen the app and choose **disconnect**.

VPN CONNECTION NOTE

While connected to VPN, all of your internet traffic passes through UF Health then back to your device. Keep this in mind while using the internet for personal use.

Please disconnect from VPN when finished using it.



CONNECT TO EMAIL

From your personal computer

You can connect to your email by visiting

UF: mail.ufl.edu

From your UF Health computer

On a UF Health computer, you can use the Outlook email client by opening the Outlook icon that is on your desktop.

FIRST TIME STARTING OUTLOOK

If this is your first time starting Outlook, choose “Next” and “Finish” on any first time setup prompts.

MOBILE DEVICE SECURITY PIN

For the best results, please have your device configured with a security pin code before attempting to setup email. A security pin is required to receive UF email on your device.

If you do not have a pin, you will be prompted to create one during this setup process.

Setup up your mobile device

1. Go to your device Settings and find the Accounts section or Mail, Contacts, Calendars section
2. Choose “add account” and select “Microsoft Exchange” as the account type.
3. Enter your email address and password, then choose Next
4. After a moment, you should be prompted to enter additional information
5. Enter the following information:

Server Name: mail.ufl.edu

Domain: UFAD

Username: your GatorLink account

Password: Enter your account password

1. Choose Next. If successful, you should see a message indicating success
 - o At this time you may be prompted to configure a device security pin
2. If the account is successfully added, go back to your home screen and then open your Mail app
3. You should find that this new account has been added and email should begin to synchronize to your device

AUTHENTICATION ERRORS

If you encounter “authentication” errors, try

- Removing or adding the Domain to the username field.
Example: domain\yourusername
- Ensure your correct password was entered and try again.

EMAIL SYNC

This initial email sync can take a couple minutes to start.



ADVANCED EMAIL

Encrypted Email

While you can confidently send restricted or sensitive information in an email from UF to UF **or** from UF to Shands, it is important to ensure restricted or sensitive information that is sent to recipients outside the organization be secured.

Sending an Encrypted Email

Sending encrypted email will work with Outlook, outlook web, and your mobile device.

Simply include in brackets, the term **[encrypt]** along with your subject in the Subject field of your email.

Example: Subject: “[encrypt] please review this soon”

Reading an Encrypted Email

Recipients of encrypted emails will receive a special email that contains a **click here** to read this message link.

Clicking the “Read this Message” link will take the recipient to the Proofpoint system website.

- If this is the recipient’s first time receiving an encrypted email, a prompt to register will appear before the recipient can open the secure message.
- Registered recipients will need to login using their registered account information.

Once logged into Proofpoint, the recipient may use the Proofpoint system to read or reply to the secure email.

Saving or forwarding secure emails from Proofpoint may not work.

Sending an eFax

A fax may be sent using your Outlook client.

From UF email

- For local numbers:
in the **To** field type:
[fax:9thephonenumber]
Example: [fax:92650526]
- For long-distance numbers:
in the **To** field type:
[fax:91thephonenumber]
Example: [fax:913522650526]

Note: the square brackets are required.

File Attachments

Most of the common file formats such as *docx, xlsx, pdf, jpg, png, txt* and more may be attached to an email.

- To protect you from malicious attack, some files such as *exe, zip, and others* will be automatically removed from the email you are sending or receiving.
- You can include files up to 35MB as attachments.



UF HEALTH CITRIX

The UF Health Shands Citrix environment is used to publish wide-use enterprise applications. There are many applications available in the Citrix environment

UF Health Shands Citrix website:

From Off-site: mycitrix.shands.org

On-site: citrix.shands.org

On your UF Health Workstation or Training computer:

The Citrix Receiver application is already installed on UF Health computers. Some Citrix applications, such as Epic, may have a shortcut displayed on your desktop.

CITRIX RECEIVER

Using Citrix applications require that a **Citrix Receiver** client be installed on your computer or mobile device.

You may want to start by installing the “Citrix Receiver” client for your respective operating system.

Please visit Citrix.com, find Downloads and choose the Citrix Receiver client that is appropriate for your operating system.

Once installed, proceed to mycitrix.shands.org and launch your needed application.

Get connected using Windows or Mac

1. Open your internet browser and visit mycitrix.shands.org
2. Login using your Shands username and password
3. Choose and click the Citrix application that you would like to use (Epic Production, etc.)
4. Once the application opens, please login

Get connected with Android or iOS:

1. Open your “app store”
2. Search for and install “Citrix Receiver”
3. Once installed, go to your home screen and open the Citrix Receiver app
4. When prompted, enter the following information and press Save

Address: mycitrix.shands.org

Username: your Shands username

Password: your Shands password

Domain: Shands

1. If login is successful, you will see an “Add favorites” notice with an arrow. Tap the plus sign to add published applications to your favorites list
2. Once added, tap the application that you want to use from the Favorites’ list
3. Once the application opens, please login



EPIC

Launching Epic

You can launch Epic HyperSpace Production through Citrix from your desktop, laptop or mobile device.

1. Login to mycitrix.shands.org and choose Epic HyperSpace Production
2. Login to Epic with your Shands username and password
3. Choose your login department

You should now be logged into Epic

Training & information for Epic

You can find training resources and up to date information for Epic at: epictrain.health.ufl.edu



STORING & SHARING YOUR FILES

Network Share Drives

You might find yourself using a UF Health computer to access data a files that are stored on Share Drives.

Network share folders are the preferred supported method for storing any of your work-related information.

File Protection

Network share folders are protected with 45 daily and 12 weekly snapshots to ensure that data is recoverable in the event of data loss.

Network Share Paths

If you have to map to a network share folder, here are the basic root paths for network shares:

For UF users:

- **Windows:** \\ahcdfs.ahc.ufl.edu\files
- **Mac:** smb://ahcdfs.ahc.ufl.edu/files

OneDrive for Business - GatorCloud

If you have a valid GatorLink account as an employee, faculty or student, you can use OneDrive.

OneDrive provides you with 1TB of cloud file storage. Cloud storage makes it easier to access files from different devices and locations. There is no need to save documents to a flash drive when traveling or using a different device.

Visit OneDrive at: <https://uflorida.onedrive.com>

Drobox for Education

Alternative approved cloud storage solutions, such as Dropbox for Education can be found at:

<http://www.it.ufl.edu/gatorcloud/>

OTHER CLOUD SERVICES

It is your responsibility to ensure that any sensitive data is secure. Using Google, Amazon, iCloud or other cloud service to store protected information is prohibited.

However, using these services to store your personal files or class information is ok.

USB drives

Using USB drives to store your personal files or class information is ok. However, if you are storing work related or files that contain sensitive information, the USB drive must be encrypted.

File-Express for large files

Use UF File-Express to share files that are too large to send in an email. Using a secure server and the GatorLink Authentication system, users can easily share files with members of both the UF and Non-UF community. File-express is located at: <https://file-express.ufl.edu>



COLLEGE APPLICATIONS

Your college will have specific applications and systems that are only used by your college.

Links

Health Science Center information
<https://ufhealth.org/health-science-center/>

College websites

- [College of Dentistry](#)
 - Student Handbook:
<https://dental.ufl.edu/files/2017/02/Student-Handbook-08022016-Class-of-2020-20170201.pdf>
 -
- [College of Medicine](#)
- [College of Nursing](#)
- [College of Pharmacy](#)
- [College of Public Health and Health Professions](#)
- [College of Veterinary Medicine](#)
 - Student Handbook:
<http://education.vetmed.ufl.edu/dvm-curriculum/student-handbook/>

College of Dentistry Systems

Education Resources:
<http://dental.ufl.edu/education/resources/>

VMWare for Axiom

You can access Axiom through VMware virtual machine environment.

Visit <https://myview.ahc.ufl.edu/>


Either install the VMware Horizon client or use HTML Access. Both are options on the front page.

Login with your account and you will see the Axiom environments that are available to you.

ECO Calendar

You can view your class schedule by adding the ECO calendar to your email apps.

Visit <http://eco.dental.ufl.edu>

1. Login with your GatorLink account
2. Navigate to the Calendar Tab
3. Find click the feed  icon
4. Copy the Feed Address
5. Follow the onscreen instructions to add the calendar to your device

Exam Soft

Beginning in 2014, the college has used Exam Soft testing software to administer selected DMD program examinations using student laptop computers. For more information about Exam Soft go to: <http://dental.ufl.edu/education/dmd-program/examssoft-procedures/>



INFORMATION SECURITY

The IT Security team works with employees to protect information systems and the confidential information that resides within them.

SECURITY ISSUES

To report a suspected information security issue, please call the IT Support Center.

General Security

- Never tell anyone your password
- Log off or lock your computer workstation whenever leaving it unattended
- Be suspicious of any unexpected emails
- If you must use the Internet at work, browse only to well-known web sites
- Save your work documents to the network drives
- If you work at home on a personally owned computer
 - install antivirus software and updates
 - set up automatic security updates
 - require a password to logon and unlock
- Make sure that your mobile devices
 - lock after no more than 15 minutes
 - use encryption
 - have device wipe enabled after 10 incorrect password attempts
 - have tracking software enabled
 - connect to the correct Wi-Fi network

Acceptable Use

UF Health information systems may only be used for authorized purposes.

- Each user is responsible for maintaining the confidentiality, security and integrity of UF Health computers and systems they use and the Confidential Information contained therein.
- Under no circumstances should UF Health systems be used for gambling, personal profit, or to download or distribute materials, comments, pictures, or other forms of communication of a sexual nature or which are otherwise obscene, intimidating, offensive, or create a hostile work environment.

Confidential Information

Confidential Information, also called Restricted Information by UF Health's Data Classification Policy, is any information protected by state or Federal law or by contract.

Examples of confidential information:

- Protected Health Information (PHI)
- Personally Identifiable Information
- Social Security Numbers
- Credit card information
- Financial records
- Passwords, PINs, or other security codes

UF Health Confidential Information can be:

- On paper
- On your work computer
- On your personal smartphone or tablet
- On a CD/DVD or USB Drive
- In a voice mail

Printed confidential information must be stored securely in a locked cabinet and shredded when it is no longer needed.

CONFIDENTIAL INFORMATION

Regardless of its form or location, you are responsible for protecting confidential information from unauthorized disclosure.

File Storage

To ensure that your work-related documents and files are appropriately protected and backed up daily, save them to the provided network drives.

PROTECT YOUR FILES

To protect your files, it is best to store them on your network share drives and not save your documents to the local internal C: drive of your computer.

User IDs and passwords

Your User ID and Password uniquely identifies you at UF Health.

PROTECTING YOUR PASSWORD

- No one should ever ask you for your password
- Never voluntarily give out your password to a co-worker, friend or family member
- Be aware of scams to trick you into disclosing your password or other sensitive information through phone calls or emails
- Passwords should be:
 - Memorized
 - Never written down so that others can see or use them
 - Kept secret from other people

Passwords Creation

A strong password is your first defense against many types of computer attacks.

The key to a good password is to not only choose something that no one will guess, but also something that is easy to remember.

UF Health passwords:

- Must be at least 8 characters or longer
- Must include at least 1 uppercase letter
- Must include at least 1 lowercase letter
- Must include at least 1 number
- May not use dictionary words longer than 3 characters
- May not contain user names, forward or backward
- May not contain more than 2 pairs of repeating characters

Email Security

Be suspicious of any unexpected emails even from a friend, family member, or coworker

Sometimes phishing and other unwanted emails reach our mailboxes.

PHISHING ATTACKS

Phishing attacks often begin with a cyber-criminal sending you a convincing email or calling you pretending to be a person or an organization you know and trust, such as the helpdesk, a friend, your bank, your favorite online store, or a charity.

- Suspect emails usually require immediate action, start with a generic salutation, and may have grammar and spelling mistakes
- Be suspicious of attachments and only open those that you were expecting
- Do not click on hypertext links, use a previously saved favorite to check something from the helpdesk or your bank. Or better yet, call a known phone number to confirm it

Web Browsing

The largest source of computer viruses comes from browsing to compromised or malicious web sites.

Practice these safe habits:

- Be careful where you browse
 - The ability to connect with a specific website does not in itself imply that it is safe.
- If you must browse the Internet, use only well-known web sites
 - Be aware that web sites of any size and popularity can be compromised
- Obtain permission from the UF Health IT before downloading or installing any software to your computer



ADDITIONAL RESOURCES

IT Training Resources

UF Health IT offers targeted training for business related desktop applications.

More information about what type of IT related training can be found at: <http://training.health.ufl.edu/>

Other learning resources

There are several places to visit for training materials.

Some of these include:

- **MyTraining**
Several UF Health related departments use myTraining to distribute learning modules.
How-to documents are available for Microsoft Office 2016 through myTraining.
- **UF IT provided training**
UF IT offers training with a valid GatorLink username

Offerings can be found at <https://training.it.ufl.edu/>

UF CAMPUS IT SERVICES

UF Health IT offers many services to you in the Health Science center colleges, Shands Gainesville and Jacksonville, and University of Florida Physicians.

Keep in mind that, University of Florida IT offers many services that are available to UF related colleges, departments, and staff.

Visit UFIT at <http://www.it.ufl.edu/>

Research Computing

UF Department of Research Computing

UF Research Computing (UFRC) staff provide HiPerGator support at no additional charge for requests such as:

- Installing software on HiPerGator
- Writing and optimizing complex submission scripts for HiPerGator jobs
- Analyzing performance problems with software or job flows within the UFRC environment

If you have any questions, would like to contact UFRC, or would like help with any HiPerGator tasks, please visit the UFRC support page: <https://www.rc.ufl.edu/help/>

UFRC also offers Linux OS support for a variety of circumstances including:

Linux Desktop Support:

- Introductory Linux training
- Workstation setup and imaging
- Operating system installation
- Software installation/troubleshooting
- Authentication setup
- Remote Linux collaboration setup

Linux Research Support:

- Linux-based file transfers
- Setup of remote applications (Xpra, X11, etc.)
- Data storage and layout
- Data flow optimizations and group access
- Permissions setup
- Lab directory synchronization on Linux

If you have any questions or would like to know more about available support options please see: <https://www.rc.ufl.edu/services/support/linux-support/>

REDCap

REDCap (Research Electronic Data Capture) is a secure, web-based application designed to support traditional case report form data capture for your research studies.

REDCap is provided at no cost for use with any research project. For those with funding, fee-based configuration services are also available to jump-start a given project

<https://www.ctsi.ufl.edu/research/study-design-and-analysis/redcap/>



SPOK ON-CALL SYSTEM

Spok is the UF Health on-call system. You may not use Spok in your program but Spok is used by clinicians (MD, PA, ARNP, Residents and Fellows).

Spok has a website interface for everyone and a mobile client for clinicians.

Spok Mobile App – Clinicians

The Spok Mobile App is a secure “texting” like application geared towards UFHealth clinicians (MD, PA, ARNP, Residents and Fellows). It provides you with a way to stay connected while juggling your schedule in clinic, the hospital, lab, or office. Whether you work days, nights, weekends, or all of the above, Spok Mobile stays with you. Installed on your personal smartphone, Spok Mobile reduces the number of devices you need to carry to stay in the loop.

Spok Mobile allows other UFHealth clinicians to “text” patient-related messages securely to you. Nurses and support staff may message you and receive confirmation of your acknowledgement without a phone call. You can even take and share photos securely within the app.

You can register your personal mobile device by following the instructions at:
<http://help.spok.ufhealth.org/clinicians/getmobileapp/>

General information and help for Spok (mobile, web and on-call) is available at:
<http://help.spok.ufhealth.org>

Spok Web – For Everyone

Spok Web is an easily accessible online directory and messaging tool that allows anyone at UFHealth to search for and securely message clinicians at UFHealth. Spok Web is geared toward nurses and staff who need to quickly, securely, and accurately send a message to clinicians.

We have imbedded Spok Web into Epic so the messaging tools you need are quickly within reach. Messages can be up to 160 characters long. A predefined message drop-down menu also provides you with frequently used phrases such as, “Consult needed...” and “Patient requests...” By sending messages from Spok Web, participating clinicians receive your message in their mobile app. A quick look in your Web message history will show whether that clinician received your message and provided a yes, no, or free-text response.

Although these tools provide the most benefit to transactions between Spok Web and Mobile, Spok Web may also be used to message clinicians who rely on pagers only.

Spok Web is available directly at:

<http://spok.ufhealth.org>

Logging in to Spok Web:

1. Enter your username with your affiliated domain first as shown:
 - **UF:** ufad\gatorlinkusername
 - **Shands:** shands\shandsusername
2. Then enter your account password



USING DESK PHONES

Using your desk phone

To place a call, lift the handset and dial as follows:

- **UF** – Last 5 Digits of telephone number
- **Shands** – 5 + 5-Digit Extension
- **Local Call** – 9 + 7-Digit Phone Number
- **Long Distance** – 9 + 1 + (Area Code) + 7-Digit Phone Number
- **International** – 9 + 011 + Country Code + Phone Number

To answer an incoming call

1. Lift the handset, or
2. Press the “speaker” button to answer hands-free

To end a call

1. Return the handset to the cradle, or
2. Press the “speaker” button if using the hands-free mode

To place a call on hold

1. While on the call, press the corresponding “hold” soft key
2. To return to the call, press the corresponding “hold” soft key again or the “resume” soft key

To transfer a call

1. While on the call, press the corresponding “transfer” soft key
2. Dial the number of the extension you wish to transfer the call to
3. When the party answers, announce that you are about to transfer a call
4. If the party accepts the transfer, press the corresponding “transfer” soft key again and hang up

Voicemail for Cisco Phones

From your desk phone perform the steps then follow the prompts

1. Pickup your personal line and press the “envelope” voicemail soft key
2. Enter your voicemail pin and press #

From outside UF Health perform the steps then follow the prompts

1. Call your phone number and wait for the voicemail message prompt
2. Press the * key to start the system prompts
3. Enter your ID which is your 5-Digit extension and press #
4. Enter your voicemail pin and press #

Voicemail for NEC Phones

From your desk phone, dial 31400 and follow the prompts

1. Enter your security code, the **First time** pass code is 12345

From outside UF Health, dial 352-733-1400

1. When the system greets you, Press * and then enter your ID (your extension number)
2. Enter your security code, the **First time** pass code is 12345

Phone Directories

You can view the following directories.

- [UF Directory](#)
- [Shands Phonebook \(GNV\)](#)
- [On-Call Schedule \(Spok\)](#)
- [Infonet Directory \(JAX\)](#)
- [On-Call Schedule \(JAX\)](#)
- [VIVO \(Research Directory\)](#)

These links are also available near the logo on the Bridge.



Laptop Protection Verification Form

Fill this out and bring to the IT Walk-up Help Desk in Communicore C2-011

Name	UFID#
College or Department	Computer Serial Number
Computer Model	Automatic Updates Enabled
OS Version	Anti-Virus Version Installed
Firewall Enabled	Whole Disk Encryption Enabled

Encryption Type (Circle)	FileVault II	BitLocker	Other
---------------------------------	---------------------	------------------	--------------

I affirm by my signature below that I agree to maintain active protection of my laptop during my tenure at the University of Florida. I will keep my Operating System and components patched; firewall enabled and maintain anti-virus and a fully encrypted hard drive. I acknowledge that disabling or removal of any of these listed items may lead to disciplinary actions.

Signature _____ Date _____

Verified By _____ Date _____

IT Service Request # _____