Best Business Practices for Setting Up a Physician's Home Office Network

By Van Pilkinton, VP of Business Development for RealTime, LLC, of Alabama.

In today's mobile world it's nice to have the ability to access your main office from outside so you can handle issues without having to leave the family or your vacation retreat when the records needed are at your practice office. The problems associated with having this convenience is that the security of accessing and storing this information in the healthcare industry is governed by HIPAA compliance guidelines.

From passwords on sticky notes to sensitive medical information left in a stack by the printer, many physicians make the same basic security errors at home as they may encounter and preach against at their practice office. The facts are that if you have access to sensitive medical records and patient information on equipment outside the primary practice office then you must treat that location as an extension of your primary office. Here are a few best practice guidelines and tips that physicians and administrators can use in helping to build a secure home office environment.

Physical Security for the Physician's Home Office Network

At the practice, you've checked all of the entry ways. You may have surveillance camera technology in place and your administrator assures you that your IT firewalls are adequate. But, have you checked your home, lake house or beach retreat for the same security vulnerabilities?

Below are a few things to add to a "must have" check list:

- ☐ Physical access restrictions; office door locks, desks and file cabinet locks.
- ☐ Secure locked access to your computers, laptops, tablets, back-up device cables, wires, power-strips, battery back-up devices.
- ☐ Fireproof lock boxes and safes for storing important documents and data back-up devices (memory sticks, external hard drives).
- ☐ A cross-cut shredder to help dispose of sensitive documents when you're done with them.

Install Business Class Network Security in the Home Office

When putting a home office together most people go to an electronics appliance store like Best Buy or Office Depot; look for a basic computer, laptop, printer and networking gear; put it together by the numbers and call it a business network.

The assumption that home office networks are not common targets for data theft or criminal access is not only wrong but can be devastating when it comes to lost medical data. The new "Home Office" for physicians must have the same fundamental security infrastructure and policy measures as their larger practice office if they want to be HIPAA compliant with access to medical record information.

Today's cyber environment changes everything that we were taught as recently as a few years ago. The average person thinks because they are at home or at the lake house, no one is going to target their network, but the contrary can be true. By configuring the network security properly, you can make it difficult enough that criminal hackers will find easier targets down the street!

A multi-tier security system is best practice that large business and enterprise corporations implement to provide different security feature sets for different security threats. A short checklist for implementing best practice security layers for a home office includes: a "commercial business strength" network firewall and a highly rated business grade antivirus/antimalware software suite that is purchased with yearly scheduled licensed subscriptions. These subscriptions keep the security software tables within the AV/AM software up-to-date in order to defend the systems against new threats being developed constantly.

It is also recommended that those households who have several personal computers in the home or retreat put a personal firewall device on any laptop/PC they are using to access medical data. This adds further

protection from infections derived from internet sources, thumb drives, CD's etc. Some Microsoft operating systems allow the owner (administrator) to activate built–in personal firewall software. If, however, you're not working with a system that already has personal firewall software embedded internally then there are other third party software and hardware options available from most major security-software vendors.

Research and choose a reputable major internet provider that services your area.

Summary points for installing your Secure Business Class Network:
- ☐ Acquire and install professional business class IT equipment including computers, laptops, printers and a secure business class data network.
- ☐ A secure Business Class Data Network includes using a reputable major internet provider that services your area.

Wi-Fi Security Access is Critical for Your Home Office

How many wireless networks can you see from your home computer? Can you see your neighbor's network? If you can see other networks from your office then you can bet that others can see your network, and possibly see and get sensitive information from your business / medical records.
Most professional network IT consultants recommend that home office networks enable some form of encryption, such as Wi-Fi Protected Access, or the newer standard of encryption known as WPA2.

Summary of key actions that are basic to protecting your Wi-Fi Security in your home office:
- ☐ Ensure your wireless router is enabled and configured for encryption.
- ☐ Most new Wi-Fi-certified devices support the WPA protocol; it is important to configure it properly.

Separate your Business & Home Networks

Best business practices for IT Security (Information Technologies Security) dictates that medical practices, clinics and hospitals segment and segregate their healthcare business networks from their public access patient networks in their facilities. The physician's home office network should follow the same best practices for security as the physician's main office network. This means separating the home "office" network from the home "family" network to be with HIPAA regulations.

Summary on key points to consider when it comes to designing the physician's home office:
- ☐ Segment and segregate the physician's home office from the home network. It doesn't make sense to make your computer more vulnerable than it needs to be by having kids playing games and others web surfing on it and

exposing it to malicious malware.
- ☐ Do not share the designated "Business PC's, laptops, tablets, printers or business data network" with family or guests in the home.
- ☐ Provide your family with computers and printers for their personal school and home projects in areas outside of the home office.

Back up Data from your Home Business Network

Finally, protecting the data at the home office by doing scheduled backups is an easy and necessary discipline just as it is at the main practice office. Power outages are major causes for losing unsaved data at work and at the home office and nothing is more frustrating than losing hours of work because of not taking a few minutes to go through a few quick back-up steps. Storms and power surges can also cause major damage and loss by destroying hard drives and network equipment when the home network is not protected by power surge equipment and battery back-up equipment.

There are several different ways to back up your computer files/data and the price range spans from under $100 per device (thumb drives, external hard drives and network attached storage) to a few hundred dollars per year for subscription cloud based back-up services.

Each method of back-up has differences in the amount of data storage provided, the type of portability, the time it takes to do the back-ups and the convenience of each associated method.

One of these solutions is to buy an external hard drive or large capacity thumb drive and to keep to a planned schedule for manually backing up data. The device should then be stored in a secure place. The problem with this plan, however, is that you may still lose information in the event of an equipment or power failure if you haven't manually backed up your latest work.

Other options include using online storage services, network-attached storage. Each of these methods are good backup technologies. It depends primarily on your budget, the importance of the data being backed up and if the data can be backed up remotely on other systems either in–house or in cloud based service facilities. The most important thing is to choose a solution that fits your needs, put a plan together and just do it!

Summary of points to consider:
- ☐ Back-up options needed to set up a secure system on the home office network:
  - o Back-up options include devices such as external hard drives, large capacity thumb drives, network attached storage and cloud based business continuity subscription offerings.

o Uninterruptible power supply (UPS) units, battery backup and commercial grade power strips are also excellent choices to enhance the security of your data. Use power strips everywhere power is needed for all devices in the event of a power failure. There are three kinds of UPS devices; standby, line interactive and online. They all provide battery backup, but they work in different ways. Determining which one you need depends on the kind of protection you require.

Final Comments

As you plan your home office it would be a good idea to use these tips as a guide and make a list of the items you currently have and those things that you may need to buy in order to make your office secure and compliant. Afterward, consult with your current practice IT services company to tweak and customize components to best fit your individual needs.

For additional information on new Home Office trends and setting up "The Home Office" go to http://www. chiefhomeofficer.com/. Jeff Zbar is the CHO and "Sherpa/ Guru" of everything Home Office!

About the Author: *Van Pilkinton is the VP of Business Development for RealTime, LLC, of Alabama. Beginning in 2000, RealTime was one of the first true IT Managed Service Providers in the country and serves clients across the Southeastern U.S. For questions and advisory on the topics of supporting the technology and the business of medicine, contact Van at vpilkinton@ realtime-it.com or call at (205) 999-9915. Website: www.realtime-it.com*

Upcoming Events

Jan. 19   The Wayne Finley 811 Breakfast Meeting – Kirby Bland, M.D., will speak at 8:30 a.m. in the JCMS Board Room

Jan. 25   Executive Committee Meeting – 5:30 p.m.
Board of Directors Meeting – 6:30 p.m.

Feb. 16   The Wayne Finley 811 Breakfast Meeting – Will Ferniany, Ph.D., will speak at 8:30 a.m. in the JCMS Board Room

Feb. 22   Executive Committee Meeting – 5:30 p.m.

Feb. 25   MASA Sixth District Caucus – 6:00 p.m.

Mar. 15   The Wayne Finley 811 Breakfast Meeting – William Castenbader, M.D., will speak at 8:30 a.m. in the JCMS Board Room

Mar. 21   Executive Committee Meeting – 5:30 p.m.
Board of Directors Meeting – 6:30 p.m.

May 22   SAVE THE DATE! Annual JCMS Barons Event – more details to follow.

Contact Juanita Pruitt at 933-8601 or jpruitt@jcmsalabama.org for more information regarding any of the above events.

2016 JCMS Board

President:	Roxanne R. Travelute, MD
Immediate Past President:	F. Cleveland Kinney, Ph.D., M.D.
President-Elect:	Katisha T. Vance, M.D.
Vice President:	Leon C. "Bud" Hamrick Jr., M.D.
Secretary-Treasurer:	Elizabeth S. Martin, M.D.
Directors:	Leland N. Allen III, M.D.
	Christina Huang, M.D. (Resident)
	Justin D. Moellinger, M.D.
	P. Jeffrey Rickert, M.D.
	Lewis R. Schulman, M.D.
Also serving on Board of Health:	Yocunda D. Clayton, M.D.
	Jennifer R. Dollar, M.D.
	Max Michael, III, M.D.
	Joshua B. Miller, D.O.
	Nicole Redmond, M.D., Ph.D., M.P.H.

2016 JCMS Ethics Committee

Danette D. Bentley, M.D.
Emily B. Casey, M.D.
Heidi R. Umphrey, M.D.
John P. Young, M.D.
Marjorie L. White, M.D.

Birmingham Area Pediatrician Needed:

Well-established practice of five pediatricians and one CRNP looking for full- or part time pediatrician for summer of 2016 or sooner.

Must be board-eligible or certified. Call nights, weekends and Saturday work shared among group. Call is supported by Children's Hospital triage line.

Competitive salary & benefits as well as a culture of work/life balance. Free-standing building with parking in good demographic area. EHR.

Reply with CV to
jhooton@totsnteenspediatrics.com
Nov. 2015

Doctors for the ASO

Medical professionals supporting the cultural, intellectual, and economic health of our community

We invite you to join your distinguished colleagues in supporting the Alabama Symphony Orchestra and celebrating two pillars of our community: medicine and the arts.

Doctor for the ASO - $1,000

Symphony Specialist - $500

Rhapsody Resident - $100

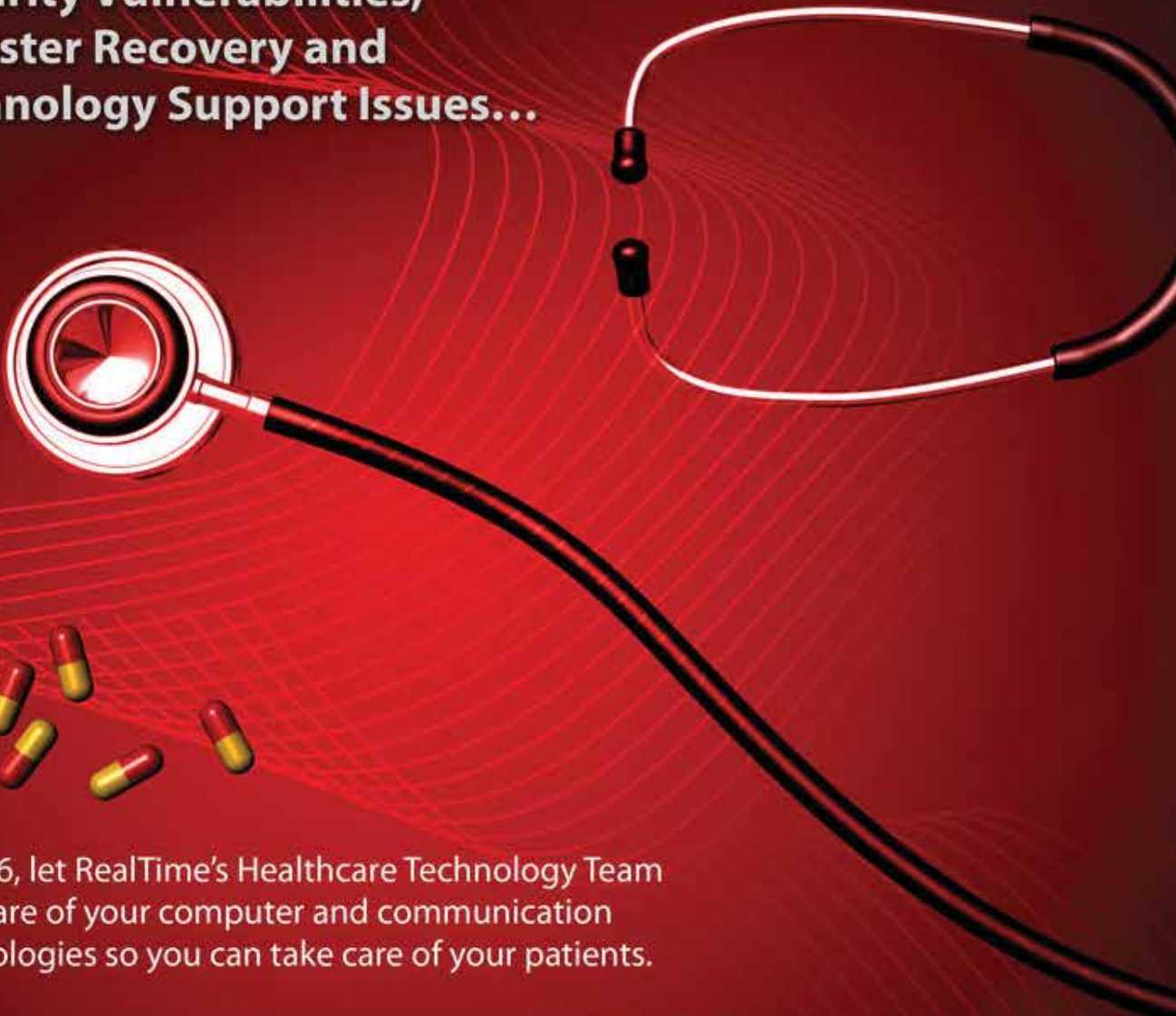RESIDENT MEMBERSHIP UNDERWRITTEN BY JOHNSON + STERLING

*JCMS MEMBERS WHO JOIN FOR THE FIRST TIME
RECEIVE A 10% DISCOUNT ON MEMBERSHIP*

Special perks include complimentary tickets, Patrons Lounge access, and an invitation to the Doctors for the ASO reception and concert on **February 6, 2016**.

To learn more or become a member, please contact Katy Smith at (205) 314-6912 or ksmith@alabamasymphony.com. You may also join online at alabamasymphony.org.

JCMS *Annual Event*

Winner of our
Hot and Hot Fish Club
gift certificate
Dr. Emily B. Casey

2015 JCMS Medical School
Scholarship Recipients

Music provided by
musician Sam Pointer

JCMS Welcomes the Following New Members

Jonathon Tyler Baccus, M.D.	Resident
Taylor M. Banahan, M.D.	Obstetrics/Gynecology
Lee Van Carroll, Jr., M.D.	Resident
Gary Chan, M.D.	Resident
Brytney Cobia, M.D.	Resident
Zachary A. Colbaugh, M.D.	Resident
John William Elliott, D.O.	Resident
Seeley Ashlyn Everett, M.D.	Resident
David H. Farrar, M.D.	Internal Medicine
Robert Foster, M.D.	Resident
Sai Gadde, M.D.	Resident
Robert C. Gish, M.D.	Resident
Warren Dale Goldstein, M.D.	Radiology
Daniel Francis Hadland, M.D.	Radiology
Beverly Harrison, M.D.	Anesthesiology
Lawrence M. House II, M.D.	Resident
Katherine Hunt, M.D.	Resident
Ayesha Jaleel, M.D.	Resident
Frederick A. Kebbel V, M.D.	Resident
Andrew M. Land, M.D.	Internal Medicine
Carole Lane, M.D.	Dermatology
Jacqueline B. Lewis, M.D.	Surgery
Jasmine Locklin, M.D.	Resident
Elyse Love, M.D.	Resident
JoBeth McCoy, D. O.	Resident
Alex Gregory McGaughy, M.D.	Resident
Adam Ross Nortick, M.D.	Physical Medicine & Rehab
Anand R. Patel, M.D.	Resident
Nishi Patel, M.D.	Resident
Joel Raborn, M.D.	Resident
Kyle William Schuller, M.D.	Radiology
Brandon Schwartz, M.D.	Resident
Mary Katherine Snider, M.D.	Resident
Jonathan Peter Southworth, M.D.	Family Medicine
David S. Summerlin, M.D.	Resident
Gregory Scott Thompson, M.D.	Resident
Jon Dezil M. Varias, M.D.	Resident
Michael Taylor Wallace, M.D.	Resident
Vivian Brooking Yeilding, M.D.	Resident
Robert H. Yoe IV, M.D.	Cardiology

In Memoriam

The JCMS wants to acknowledge the recent passing of the following JCMS members:

Robert Ellsworth Jones, Jr., M.D.
November 7, 2015

John T. McCarley Jr., M.D.
November 23, 2015

POWER

CONTROL

+

HELP

When you need it.

*Medical professional liability insurance specialists
providing a single-source solution* | **ProAssurance.com**

PROASSURANCE
Treated Fairly

PROASSURANCE.
Treated Fairly

Jefferson County Medical Society

901 South 18th Street
Birmingham, Alabama 35205