

## Protecting Patient Health Information on Your Mobile Device

With the changes in today's health care industry, the Health Insurance Portability and Accountability Act (**HIPAA**) plays an important part in the patient-physician relationship. Patients acknowledge and can give permission for the disclosure of their health information needed for their care, however, they also place a fair amount of trust in their physicians and hospitals to keep their information protected.

With the introduction of mobile devices being used in healthcare today, issues regarding the safeguarding of **PHI (protected health information)** have come to the forefront. If you or your staff frequently use a mobile device such as a **Smartphone, IPAD** or something similar, do you know the necessary steps needed to protect **PHI**?

### Use a password or other user authentication

Mobile devices can be configured to require **passwords** or **PINS** to gain access to it. A strong password should be something easy for you to remember and contain at least 6 characters, with upper and lowercase letters and a punctuation mark or other keyboard character. Change your password often, and do **NOT** store your passwords in an easily accessible place. Your mobile device should also be set to **lock** after a period of inactivity, thereby preventing an unauthorized user from gaining access to it.



### Install and enable encryption

It is extremely important that you encrypt the data that is both stored locally **ON** your mobile device, (data at rest) as well as data **SENT** by your mobile device (data in motion). Encryption methods will vary with each device, and you may need to research your device's encryption capabilities. If your mobile device does not come with built in encryption, you should research mobile applications carefully

before you download one to your device. Make sure you are able to verify that they come from a trusted source.

### Install and activate Remote Wiping and/or Remote Disabling

Remote wiping is a special security feature that enables you to remotely erase the data on the mobile device in the event it is lost or stolen. When you enable a remote wipe feature on your mobile device, you have the ability to permanently delete the data stored on it. Remote disabling allows you to remotely "lock" your device to prevent unauthorized use of it. Check for these features on your mobile device, or research the available applications (apps) before downloading them to your device.

### Disable or do not install or use file sharing applications

File sharing applications enable others to access your laptop without your knowledge. They can access private information or place a virus on your system. Disabling file sharing will reduce a known risk to data on your mobile device.

## Meet Our Experts

Periodically, we will be taking the opportunity to introduce you to one of our valuable staff members so you can get to know the people who work "behind the scenes" here at **CRT**. We call them "our experts", but if you are a client of **CRT's**, they are **YOUR** experts too! We appreciate each and every one of them.



**Shirley Crozier, Account Leader**

**How long have been employed with CRT?** 9 years

**How long have you been in the medical billing industry?** 31 years

**Personal:** Married 40 years. I have two children and one grandchild, and I enjoy reading in my spare time.

**What do you find most challenging about your job?** The changes in the insurance industry and keeping up with all of them! You have to be persistent to be in this business.

**What do you consider your biggest career accomplishment?** I went in front of a Medicare Administrative Law Judge along with an ENT physician I worked for, to convince them of the medical necessity of a specific test. I had stashed and appealed this claim for two years, before the judge finally **agreed** that this test should be covered by Medicare. It was very satisfying to finally get this physician the reimbursement he deserved!

**Motto:** **NEVER** give up! I apply this to both my personal and professional life.