Apple iOS 5 Security Requirements

Apple's release of iOS 5 includes new features and applications (*apps*) that bring added access convenience and fun to iPhones, iPads and iPod Touches…but it also raises new concerns about information security. Protecting PHI, CHI confidential or other sensitive information is of major importance at CHI and because of the need to protect this data, there are some settings and functions that require your attention. The requirements are listed below.

The CHI Enterprise IT Security team is actively working to enforce security parameters in the coming months. In the meantime, it is important for CHI users to apply these security parameters in protecting PHI and CHI confidential information.

iOS 5 FEATURE	EXPLANATION

iCloud	**What Is It?**
	• Apple's iCloud is a unique brand of "cloud" services that's geared more toward personal use than professional use.
	  ◦ iCloud uses a free cloud data storage service (Internet) to store/backup your music, photos, documents, and other data and wirelessly pushes them to all your devices.
	  ◦ If you buy a song, take a photo, update a document or edit a calendar event on your iPad, iCloud makes sure it appears on your iPhone, iPad, iPod touch, Mac or PC.
	• iCloud gives you access to your information from whichever device you happen to be using, keeping your email, contacts, calendars, notes, photos, documents and iTunes music/videos/other media up to date across all your devices that use iOS 5.
	
	What's the Risk?
	If you use your iPhone or iPad (with iOS 5) to access any CHI information (emails, contacts, calendars, documents, images, audio files, etc.) there is a potential risk that some of this data may be stored on a non-CHI device.
	
	What Action Should I Take?
	
	***CHI-Issued Devices*:**
	
	Users of CHI issued devices (iPhones, iPads, and iPod touch) **must not enable iCloud service.** Please go to Settings>iCloud to ensure that the iCloud settings are turned **"OFF"** for all the services including Mail, Calendar, Contacts, Documents and Data

iOS 5 FEATURE	EXPLANATION

	▪ ***Back Up to iCloud*:**
	  ▪ Set iCloud options to **OFF**.
	  ▪ This setting controls the ability to automatically back up your Camera Roll, accounts, documents, and settings to an iCloud Internet/personal data storage site.
	▪ ***Personally Owned Devices:***
	Users with iPhones, iPads, and iPod touch devices who use their devices to access CHI email, contacts, or calendar must ensure that the iCloud settings are turned **"OFF"** for Mail, Calendar, Contacts, Documents and Data services. ***iCloud settings for synching mail, contacts, calendar, reminders,*** documents and data**:** Set these options to **OFF**.
	  ▪ This setting will protect against emails, contacts, calendar and documents containing CHI data from being synched to an *iCloud* Internet/personal data storage site.

Notification Center 	**What is it?** With Notification Center, you can keep track of notifications all in one convenient location. New notifications appear briefly at the top of your screen, without interrupting what you're doing. And the Lock screen displays notifications so you can act on them with just a swipe. **What's the Risk?** If you use your iPhone or iPad (with iOS 5) to access any CHI information (emails, contacts, calendars, documents, images, audio files, etc.) there is a potential risk that CHI calendar notifications, reminders, missed calls and messages may appear briefly at the top of your screen. **What Action Should I Take?**  ***CHI-Issued Devices or Personally Owned Devices:*** Users of CHI issued devices (iPhones, iPads, and iPod touch) must **disable** notifications for Reminders, Messages and Calendar. Please go to **Settings>Notifications** to ensure that the "**View in Lock Screen**" settings are turned **"OFF"** for Messages, Reminders and Calendar settings. ▪ ***View in Lock Screen*:** ▪ Set this option to **OFF**. This prevents message preview when the screen is locked.

iOS 5 FEATURE	EXPLANATION

Find My Friends 	**What Is It?**
	• Find my Friends is an application that tracks where your friends are located via GPS.
	  ▪ The application can be downloaded from Apple Application Store.
	• If you accept someone's Friend request, they will then be able to track your location, too.
	• If your friends or other contacts give the OK, you can see their current whereabouts on a map—and vice versa.
	
	What's the Risk?
	Find My Friends application allows anyone who is designated as a "friend" to locate a user or his/her iPhone or iPad. That could be a prelude to theft. Find My Friends could also be used to covertly monitor a user during off hours, which—beyond being an invasion of privacy—could open someone up to blackmail or other forms of coercion.
	There are privacy issues regarding tracking someone's location. Who has permission to track you?
	  ▪ Do you trust everyone you include in this application?
	  ▪ Could you have included someone that you don't know very *well* and who may not have your best interests at heart? Do you want that person to be able to track you?
	• Do you really want to be located all of the time?
	  ▪ Find My Friend works with your Contacts and Maps, so it's easy for someone to find your location.
	
	What Action Should I Take?
	 
	
	***CHI-Issued Devices*:**
	Users of CHI Issued devices ((iPhones, iPads, and iPod touch), **must not use this application due to potential privacy impacts**.
	
	***Personally Owned Devices*:**
	Due to the potential privacy impacts, if users download and set up Find My Friends on an iPhone, iPad or iPod touch device, we highly recommend that the **users exercise extreme caution** about who is allowed to follow you.

iOS 5 FEATURE	EXPLANATION
Siri 	**What Is It?** The Siri application is integrated into iOS 5 and it has at least some level of access to all of Apple's built-in iOS apps, including Mail, Messages, Calendar, Notes and so on. ▪ Siri talks to you and allows you to talk with it. ▪ It's a voice recognition application that uses Wi-Fi networks and lets you use your voice to send emails, schedule meetings, place phone calls, and more—all that without having to type in instructions. ▪ Siri also reads to you, instead of you having to read information yourself. **What's the Risk?** The risk is being overheard if dictating or listening to patient or other CHI confidential information. ▪ Who is around when you are talking or listening to Siri? ▪ Do you discuss patient information or CHI business, confidential or internal, with someone when using Siri? ▪ Do you use Siri to dictate information that should be kept private? Can other people hear what you say? Are you sure? ▪ Another potential risk is that Siri may be activated even when the iPhone is locked, potentially giving someone other than you, the owner, some level of access. **What Action Should I Take?**  ***CHI-Issued or Personally Owned Devices***: **Never use this application when listening to or dictating PHI or CHI confidential information in a non-private location.** ▪ Be aware of your surroundings! Remember that people who are sitting near you may hear CHI confidential information.

iOS 5 FEATURE	EXPLANATION
iMessage 	**What Is It?** • iMessage provides the ability to exchange unlimited text messages, photos, videos, locations and contacts to all iOS 5 users via Wi-Fi or 3G from your iPad, iPhone, or iPod touch to anyone with one of those devices. • iMessage also provides the ability to message groups and to see when someone is typing a message. You can even start a conversation on one iOS 5 device and finish it on another. **What's the Risk?** The risk is ensuring that everyone you send CHI confidential information or other CHI related information to has the authorization to receive it. **What Action Should I Take?**  ***CHI-Issued or Personally Owned Devices***: iMessage application **must not to be used for communicating any PHI or other CHI confidential information.**

iOS 5 FEATURE	EXPLANATION

Smart Cover
 
	What Is It?
	• Smart Cover protects an iPad 2 screen and, when removed from the screen, it can act as a stand or it can be folded back like the page of a magazine.
	• Removing the cover can also "wake up" the iPad.
	
	What's the Risk?
	• The risk is a "bug" about how iOS 5 handles the Smart Cover that makes it possible to bypass the iPad's passcode screen. The bug generally seems to affect iPads running iOS 5, but the issue is present on some that are still running iOS 4.3. While someone may be able to get onto your iPad using this trick, they will only be able to get at whatever application you happen to have open.
	• What was open on the screen when you locked it?
	  ▪ Was it your CHI email, or your calendar, or contacts?
	  ▪ Was a confidential document visible or had you been listening to an audio file with patient information when you locked the screen and someone accessed it?
	  ▪ Was Safari open? The individual could navigate anywhere using Safari, including to infected or malicious sites.
	• Although someone who accesses a locked iPad 2 (iOS 5) with a Smart Cover on it cannot open any new applications, the risk of someone accessing CHI confidential information from an application that is open is real.
	
	What Action Should I Take?
	 
	
	CHI-Issued Devices:
	
	Apple is addressing the security concern as part of their upcoming security fixes. CHI will issue the security patch notification and work with CHI iPad users to ensure that the security patches are applied to CHI issued devices. The users must be aware of this security issue and take proper care in protecting the devices in public places, meetings and conferences.
	
	Personally Owned Devices:
	
	If your iPad 2 has access to any PHI or other CHI confidential information, you must ensure that the security fixes are applied to your iPad devices in a timely manner. The users must be aware of this security issue and take proper care in protecting the devices in public places, meetings and conferences.

iOS 5 FEATURE	EXPLANATION
FaceTime 	**What Is It?** ▪ Using the built in cameras, FaceTime allows users to make video calls from an iPad 2 (with iOS 5) or iPhone to another user's iPad 2, iPhone, iPod touch, or Mac using Wi-Fi networks. **What's the Risk?** The risk is being overheard or non-authorized individuals seeing PHI or other CHI confidential information that is being communicated. ▪ The information may be communicated verbally or visually with the camera. **What Action Should I Take?**  ***CHI-Issued or Personally Owned Devices***: **FaceTime is not to be used for communicating any CHI related information**.

Note: All Apple product graphics used in this document are registered trademarks of Apple Inc.