ArcSYS, Inc.- Draper, Utah

Volume 15, Number 11

November 1, 2014

ArcBITS Newsletter

Inside this issue:

MozyPro Saves the Day

This is a story which could have had a very different ending. Fortunately, this client had opted to utilize the backup service known as MozyPro for their offsite data storage. Unfortunately, they had become infected with malware known as CrytoWall which demands the payment of $500 to recover your encrypted data. The payment is demanded using TOR and Bitcoins in order to maintain the recipients' anonymity. Malware researchers strongly advise against paying the CryptoWall Ransomware ransom.

It all started on a Thursday when "some version of Skype" was being installed on one of the pc workstations within the office. Now if you have ever installed software on a pc, you have an idea of how many buttons need to be clicked here, checked there, and then presto, your software is installed. But, what you don't know for certainty, is if you are in the right web site.

We suspect that some link led to some button which then led to CryptoWall getting downloaded. Once this program was installed, it started to look for all folders that this pc had access to. If it found a .doc or .pdf file, for instance, it ran an encryption on the contents of the file. Then it would move to the next file and repeat the process. Over the space of 12 hours this nasty little program had rendered over 150,000 files as being useless including files on a separate image server!

It didn't become apparent that there was a problem until one of the users tried looking at a previously scanned document that was associated with a patient. Adobe came up with an error message saying it couldn't read the file. An attempt was made to look at another patient's scanned documents. Same result. They couldn't be read, either.

ArcSys became involved on Monday and we weren't sure what the real underlying problem was. In looking in the Windows Explorer folders where these files were stored, there was no indication that anything had been changed. We then discovered files in the infected folders that had "decrypt" instructions.

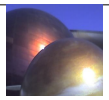
We decided it would be a good idea to look at what MozyPro had stored. At this point it was noticed that MozyPro thought there was a file change made just a couple of days earlier. Because MozyPro keeps a ***full image of all your backed up files for EACH of the past 90 days***, it was "easy" to instruct it to recover data from the Wednesday just before the pseudo-Skype install had occurred. Disaster averted. It took about 18 hours to recover all the data. Mvbase and Red Planet were unfazed by this attack.

Moral: 1) Keep your anti-malware and anti-virus software up to date. 2) Have very strict guidelines on who can install software. 3) Lastly, remember that no one is immune from the Internet cyber bullies.

ArcSys Hot Tip

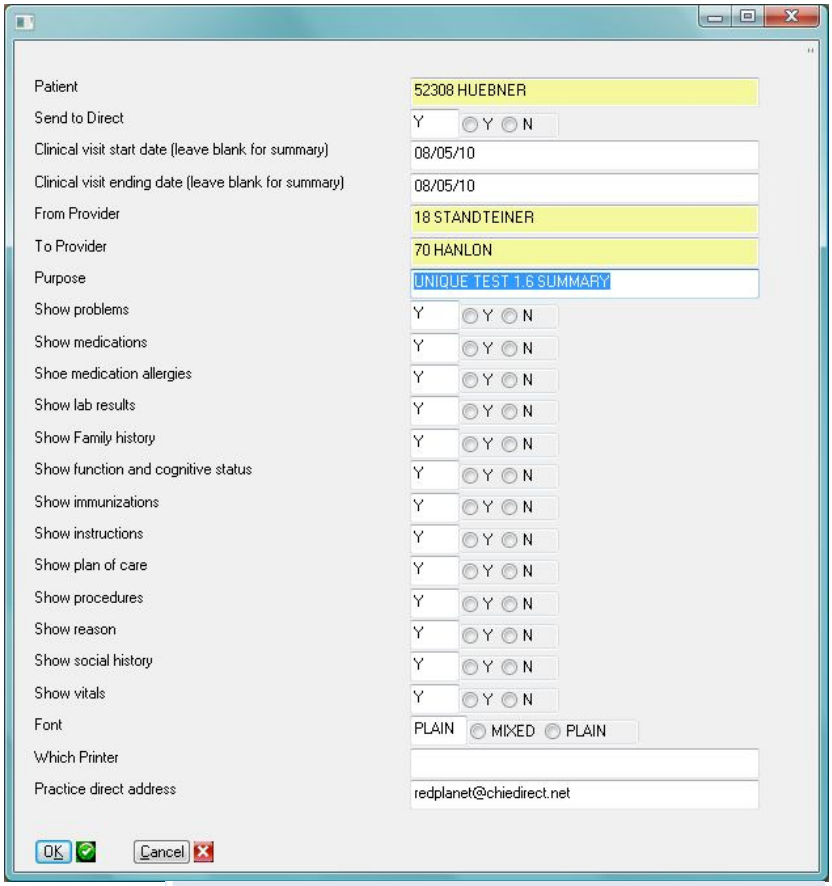
Deadline for ICD-10 Allows Health Care Industry Ample Time to Prepare For Change

The U.S. Department of Health and Human Services (HHS) has issued a rule finalizing **Oct. 1, 2015** as the new compliance date for health care providers, health plans, and health care clearinghouses to transition to ICD-10. This new deadline gives providers, insurance companies, and others in the health care industry time to ramp up their operations to ensure their systems and business processes are ready to go on **Oct. 1, 2015**.



What is Direct?

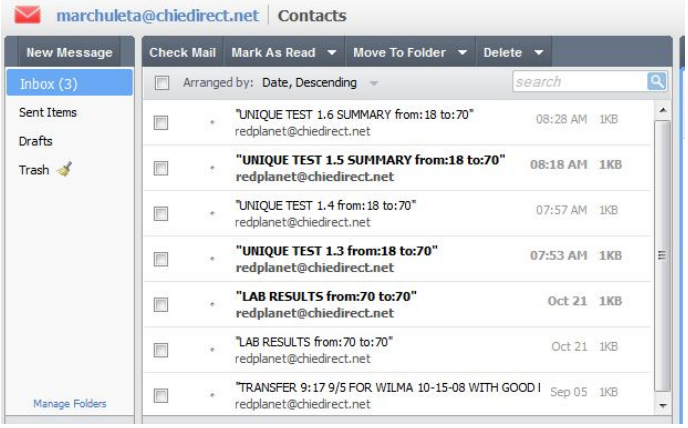
One of the features of Meaningful Use 2 is the ability to send and receive patient medical records electronically between medical providers utilizing different computer systems. This is handled through a schema known as Direct. ArcSys has partnered with UHIN/cHIE, Crosslink Software, and Secure Exchange Solutions to provide this sophisticated functionality.



Let's look at it from the point of view of your provider wanting to send a medical record. The first thing that needs to be known is the "direct address" of the receiving provider. This looks like any regular email address such as *drkathywilliams@chiedirect.net*. From within the Red Planet dashboard screen is a button called Direct and this will bring up a screen (shown on the right) giving you the option to indicate what you want to send. There are two type of things that are normally sent: A visit note for a given date(s) or a summary record. Once the Ok button is clicked, a computer file is prepared, written to a folder, and then behind-the-scenes software takes over. This extra software encrypts the file, contacts the intermediary, and leaves the file in a place where the receiver can pick it up.

The receiver is first notified that they have received a record in their regular email. The message received there tells them to log into the secure email server.

In our case, the recipient would log into their secure email account @chiedirect. Once logged in, they click on the received message. A notification is then sent



back to the sender that the recipient has opened the message.

After opening the received message, the recipient has the option of blending medications, allergies, and problem list items into their own medical record.