# The DHIN Dialogue

April 2017

A Newsletter from the Delaware Health Information Network

DHIN
Delaware Health Information Network

## Successful St. Francis Conversion to Cerner Compass

Eighteen months of work wrapped earlier this month, when Delaware Health Information Network (DHIN) partnered with the team at St. Francis Healthcare to support the health system's successful conversion to the Cerner Compass EMR.

In addition to feeding the Community Health Record, St. Francis Healthcare is also submitting data through Compass to support:

- The exchange of admission, discharge and transfer information with Maryland's health information exchange, CRISP
- Event notifications for subscribing clinicians and ACOs
- Health Check Connect, DHIN's personal health record for patients

While it appears any lingering results delivery issues have been addressed, please continue to check the volume of results from St. Francis hitting your EMR to ensure you are receiving what you need. Your practice should have another DHIN channel (Inbox or AutoPrint) against which to reference and reconcile the results hitting your EMR.

Congratulations to the St. Francis Healthcare/Trinity Health teams, and kudos to DHIN project lead **Patrick Schliesing** and technical resource **Jonathan Val** for their efforts in ensuring a smooth transition for St. Francis results delivery.

## Secure Messaging with DHIN's Directory

As part of our ongoing efforts to improve communication between healthcare providers, DHIN has launched a provider directory for secure messaging. You'll find a link to the directory on dhin.org, next to the Community Health Record link.

The directory, which will be updated regularly, lists secure email addresses for participating Delaware physicians, to be used to safely exchange patient information, per ONC requirements.

Only DHIN-enrolled users can access the directory. Just enter your user ID and password as you would for the Community Health Record to view the directory.

To add your practice's secure address to the directory or to establish a HIPAA-compliant secure address for your practice, please contact your DHIN Relationship Manager or the DHIN HelpDesk at helpdesk@dhin.org.

There is no charge for this service through June of 2018. We hope this directory saves time and makes secure exchange easier for you and your practice.

## DHIN Data Pool Deepens!

**Medical Diagnostic Laboratories** has joined DHIN as a data sender, supplying lab and pathology results for patients from Delaware, Pennsylvania, Maryland, New Jersey and New York.

More data on more patients from more places makes DHIN's Community Health Record even more valuable!

## Number Crunching...

99%

DHIN is thrilled to share that 99% of Delaware licensed providers who make orders are now signed off with DHIN!

And, as we shared in the March issue of the *DHIN Dialogue*, the number of patient care summaries available in the Community Health Record now totals more than one million from over 100 practices and 400 providers!

Viewing them is easy – we'll walk you through the process in this short video!

## Tech Tips

*For answers to commonly asked questions or technical problems, be sure to visit our Tech Tips page on the DHIN website, under Resources. Included are links to commonly viewed instructional videos, which may help you solve occasional Community Health Record challenges. As always, please feel free to contact our HelpDesk at helpdesk@dhin.org or (302) 480-1770.*

## Steer Clear of Online Safety Hazards

DHIN's Network & Operations Manager **Jody Wilson** shared these online safety suggestions with the DHIN team recently, and we thought they were worth re-sharing here.

**Obtain comprehensive security software.** Be sure that your security software protects you and your PC from viruses, worms, Trojans, spam, phishing scams and other malicious software. It should also have a firewall, which can monitor your Internet connection and stop unwanted traffic to and from your PC. Be sure to keep your security software up-to-date. Ideally, it should have automatic updates and upgrades.

**Share your email address with only trusted sources.** If you post your email address on websites, forums or in chat rooms, you are vulnerable to receiving spam or having your email passed on to others. If you would like to subscribe to a newsletter or website or receive confirmation email for online transactions, consider using a generic email address that is not linked to any of your personal information, i.e. giraffe@sampleemail.com.

**Open attachments and download files with caution.** You can get a virus, worm or Trojan simply by opening email or attachments, or by accepting files from senders, including your friends and family. If you choose to download files, make sure your security software is enabled and pay attention to any warnings provided.

**Be smart when using IM programs.** Protect yourself by using a nickname for your IM screen name. Never accept strangers into your IM groups. Be cautious about how you use your personal IM at work as your employer may monitor and view your personal messages.

**Watch out for phishing scams.** Phishing scams use fraudulent emails and fake websites, masquerading as legitimate businesses to lure unsuspecting users into revealing private account or login information. If you receive an email from a business that includes a link to a website, check that the site is legitimate by opening a separate web browser and visiting the URL directly. You can also verify that an email is, in fact, from a legitimate business by calling the business or agency directly.

**Use email wisely.** Even if you have good security software on your PC, your friends and family might not have the same protection. Be careful about what information you submit via email. Never send your credit card information, Social Security number or other private information via email.

**Do not reply to spam email.** If you don't recognize the sender, don't respond. Even replying to spam mail to unsubscribe could set you up for more spam.

**Create a complex email address.** A complex email address makes it more difficult for hackers to auto-generate your email, send spam or target your email for other types of attacks. Try to use letters, numbers and other characters in a unique combination. Substitute numbers for letters when you can, like Tracy3Socc3r2@sampleemail.com.

**Create strong passwords.** Make it difficult for hackers to crack your password. You can create a smart password by incorporating capital letters, numbers, special characters and using more than six characters, i.e. Go1dM!n3.

**Never enter your personal information into a pop-up screen.** Sometimes a phisher will direct you to a real organization's website, but then an unauthorized pop-up screen created by the scammer will appear, with blanks in which to provide your personal information. If you fill it in, your information will go to the phisher. Install pop-up blocking software to help prevent this type of phishing attack.

## Getting in Touch- DHIN Relationship Managers

**Ed Seaton**
New Castle County practices
ed.seaton@dhin.org

**Garrett Murawski**
Kent County and Bayhealth practices
garrett.murawski@dhin.org

**Michael MacDonald**
Sussex County, PRMC, Atlantic General Hospital and Beebe Healthcare practices
michael.macdonald@dhin.org

**Jamie Rocke**
St. Francis, Union Hospital and Nemours practices
jamie.rocke@dhin.org

**Lakeisha Moore**
Christiana Care practices
lakeisha.moore@dhin.org

## Staying Social

Like. Follow. Tweet. Share. **Connect with DHIN.**

Like our enrollment numbers, DHIN's social media presence is growing!
In fact, we aren't aware of another HIE with as much of a following on Facebook - thanks to all those who have "liked" us!
**5,000+ followers and growing**!