

COMPLIANCE CONNECTION

INSIDE THIS ISSUE:

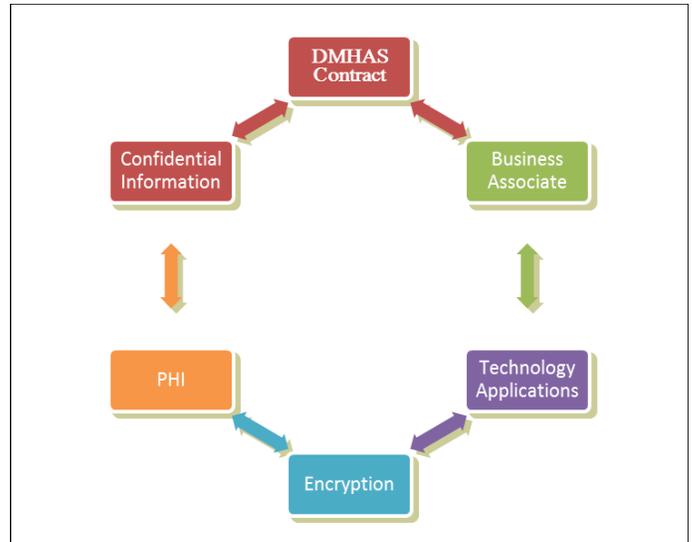
<i>Contracts and BAA</i>	1
<i>Email and Encryption</i>	1
<i>News you can Use</i>	2
<i>What's in a Number</i>	2
<i>References & Contact</i>	2

Special points of interest:

- Who are your business associates and when do you need a Contract?
- Steps on how to encrypt your documents for email
- Compliance in the news
- Numbers . . . What do they mean and why do we care?

CONTRACTS AND BUSINESS ASSOCIATES

Who are your business associates? Any person or entity who either provides services on behalf of a Covered Entity or to a Covered Entity which involves the use or disclosure of (PHI) protected health information AND is NOT a member of your workforce. They typically perform a function on behalf of the Covered Entity that involves the use or disclosure of PHI. Workforce is exempt (students, residents, volunteers). Examples of a Business Associate could be computer consultants with access to PHI, clearinghouses, third party billing services, accounting and auditing services, other consulting services, financial services, just to name a few. Who are NOT Business Associates? Post Office, CMS oversight agencies, Providers with staff privileges. The easy question to ask is – do they need access to PHI to perform their job? If yes, consider that they could be a Business Associate and must have a DMHAS contract to have access to client data. Remember that PHI is “individually identifiable health information that is transmitted or maintained in



Examples of when a Contract is needed

any form relating to the past, present or future physical or mental health condition of an individual; or provision of health care to an individual OR payment for the provision of health care to an individual.” There are 18 identifiers that are deemed PHI. Most business associates with DMHAS have a Contract wherein our Business Associate language is embedded in their contract. It could also be

in the form of a Memorandum of Agreement or a Memorandum of Understanding. Please remember that if you are considering doing business with an outside entity you must have a contract or BAA to do so. Contact Liz Taylor Chief Compliance Officer (860.418.6648) or your facility compliance officer if you have a question or need more information.

EMAIL AND ENCRYPTION . . . TAKE TWO

A reminder that when sending PHI (protected health information) or confidential/ sensitive information (social security number for example) in an email you **MUST** always **encrypt the document** before inserting it in the email. Outlook email is only as secure as you make it. The steps are quick and

easy. When your document is in Word, Excel, Powerpoint:

1. Click “file” and “protect workbook”
2. Click on “encrypt with a password”
3. A “Password” window will open – Enter a password (of your choosing)
4. “Reenter Password” then

Click OK. That’s it – You’re done—mission accomplished!

Now, call the recipient and tell them the password. **NEVER** send the password in email! For information or assistance contact the Help Desk at 860.262.5058. We’re here to help!

NEWS YOU CAN USE . . .

SNOOPING ST. CHARLES HEALTH SYSTEM EMPLOYEE FOUND TO HAVE ACCESSED ALMOST 2,500 PATIENT RECORDS

DA launches criminal investigation into actions of a “curious employee...”

The four-hospital St. Charles Health System in central Oregon had discovered an employee accessed the medical records of almost 2,500 patients without authorization or a legitimate work reason to do so, over a period of 27 months from October 2014 to January 2017. The employee claimed to have accessed medical records out of curiosity. The health system acted swiftly and launched an investigation; the employee was disciplined. The health system stated that they did not consider the employee’s actions to be criminal in nature

and a signed affidavit was obtained in which the employee stated she had not used or shared any of the information with others for the purpose of committing fraud, financial crimes or any other crimes against the patients concerned; the incident was reported to HHS OCR and state regulators as appropriate.

However, Deschutes County District Attorney John Hummel believes law enforcement should have been notified of “an alleged breach of that

magnitude,” to allow a criminal investigation to be conducted. The DA has now launched a criminal investigation into the case and will work with the police department to determine if any laws were broken. If that’s the case, criminal charges will be filed against the employee.

Remember that violation of HIPAA may result in civil monetary fines and/or jail time for knowingly violating the rule. Safeguard our client information, don’t be tempted to snoop!

WHAT’S IN A NUMBER?

“... 69% of breaches are due to employee negligence...”

According to the OCR (Office of Civil Rights) from January 2016 to November 2016 there were approximately 169,013,996 people affected by 1,737 healthcare breaches. The Ponemon Institute (those folks who gather and analyze data) further studied the data and warns that the threat for a data breach in healthcare is very real. Here are some of the numbers and

what they revealed:
Criminal attack = 50%
Medical Identity Theft = 38%
Employee Negligence = 69%
(some numbers counted in <one category)

So what ‘s in a number? And what does it mean to us??

Information and lessons learned from the healthcare industry warns us to shore up

our internal processes . Remember *Compliance is every-one’s job*. Be sure you encrypt your email, do not leave PHI unattended, use confidential locked transport bags when appropriate and use designated shred containers for PHI. *Less is more (Minimum Necessary Rule)* — use, access and disclose only what is needed to do the job and safeguard all PHI!

REFERENCES

<http://www.lagrandeobserver.com/newsroomstafflist/5160553-151/da-launches-criminal-probe-into-st-charles-breach>

Ponemon Institute, *Sixth Annual Benchmark Study on Privacy and Security of HealthCare Data*, May 2016

Chief Compliance

Officer:

**Elizabeth Taylor, OOC,
860.418.6648**

Do you have a topic of particular interest you would like to know more about? If so, please contact me (above) or send an email to elizabeth.taylor@ct.gov

Facility Compliance

Officers:

Ellen Brotherton, WCMHN
Tracey Edwards, SMHA
Megan Goodfield, RVS
Gretchen Mrozinski, CMHC
Marlana Rugg, CRMHC
Sue Wrubel, CVH
Paula Zwally, SCMHS

**To report anonymously: Compliance Hotline: 860.418.6991 | Toll free: 877.277.9471
Privacy Hotline: 860.418.6901**