Greetings,

Welcome to Winter! I wish you a blessed holiday season. Be safe, relax and spend time doing something that you love.

This Association is committed to sharing information that will assist you in your professional career development and allow you an opportunity to network with your peers.

Quarterly meetings are held in Winston-Salem, North Carolina or at a vendor’s place of business. Please see the specific brochure for each meeting.

In April, 2017, we will hold our annual meeting at the beautiful Myrtle Beach Hilton in South Carolina. We invite all members from every state to join us. If you are not a member, we invite you to become one!

*Lana L. Heecher*,
NCAHCSN-President 2016
Objectives:

Define PHI
Define HIPAA
Identify ways in which an employee may be out of compliance with HIPAA
Discuss consequences of violating HIPAA in the workplace
Discuss ways to stay in compliance with HIPAA

What is PHI?

Ted has his annual physical examination at Dr. Talk-A-Lot’s office. Ted walks in feeling healthier than ever. After his examination, Dr. Talk-A-Lot notices that his lab values are abnormal. He orders additional lab test and, furthermore, wants Ted to have an ultrasound completed. Dr. Talk-A-Lot stumps into the lobby, packed to capacity with patient’s waiting to be seen and screams out, “Nurse Betty, it does not look good for Ted, I believe he has cancer, and it does not look like his insurance is going to cover his treatment”! Shocked, patients begin looking at one another feeling intimidated. One patient whispers to the next one, “I do not want all of these people to know what I am being seen for”. Did Dr. Talk-A-Lot have the right to expose Ted’s private health information? Was his actions ethical? Did he violate Ted’s privacy? A patient’s personal health information should be concealed. Think about it, let’s say that you have been diagnosed with some type of ailment that you have not had the opportunity to properly process for yourself. Would it be acceptable for your physician, nurse, nurse’s aide, surgical technician, sterile processing technician, or any other health professional to expose your personal health information without your consent? Would it be appropriate for them to uncover your private health information (PHI) with your consent? The answer is no! PHI is an acronym that stands for Protected Health Information. PHI can include any of the following as described by True Vault (2016):

- Data in a medical record that identifies an individual
- Data that was created, used, or disclosed in the course of providing a health care service or procedure such as blood test results, MRI scans, etc., that personally identifies an individual
- Data that releases a diagnosis or treatment identifying a specific individual
- Data listed in medical records that identifies an individual
- Conversations amongst medical professionals discussing treatment of an individual
- Personal billing information of an individual

These are just a few examples of PHI. According to Rouse (2015), PHI can be defined as “demographic information, medical history, test and laboratory results, insurance information and other data that a healthcare professional collects to identify an individual and determine appropriate care”. Not only is the way Dr. Talk-A-Lot reacted unethical, it is unlawful. We will discuss reprimands for his actions later. There is another type of PHI medical professionals should also be concerned about that comes in the form of any technical or electronic record known as ePHI. Electronic Protected Health Information (ePHI) is the release of individually identifiable health information through desktops, web, mobile, email, text messages, and other electronic sources (True Vault, 2016). Regardless of the mode of transmission, protected health information should remain protected and under no circumstances be compromised.
What is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) was created as a national set of standards in 1996 to protect, keep confidential and secure the transfer of personal health information (Zabel, 2016). All facilities must follow HIPAA regulations. Regulations are variant from standards. Regulations are those that are governed and must be followed to be in compliance with the law. Standards are not necessarily governed. When we discuss HIPAA, we are outlining two rules, the security and privacy rule. Contained in the HIPAA Privacy Rule, an established set of national standards were created to protect individuals’ personal health information, PHI, and/or ePHI. The HIPAA Privacy Rule requires that specific safeguards are set to protect the privacy of personal health information, and within these safeguards, limits the uses, conditions, and disclosures of how personal health information is established (U.S. Department of Health and Human Services, 2016). In addition to the rules contained in the HIPAA Privacy Rule, patients are allowed the right to request modifications to any inaccuracy’s displayed in medical records, and are allowed to obtain a physical record of their PHI through the appropriate request of those records. Patients also have a legal right to request reports of when and why their medical records were shared with others clinics or departments for any given purpose as covered under the Privacy Rule. “The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called “covered entities” must put in place to secure individuals’ “electronic protected health information” (e-PHI) (U.S. Department of Health and Human Services, 2016)”. To address this term in simplest form, the Security Rule is basically responsible for establishing standards on a national level to secure patient data that is either stored or distributed through any electronic medium. The HIPAA Security Rule requires specific safeguards to ensure compliance. These safeguards include: Administrative, Physical, and Technical. Administrative safeguards ensure that expected or unexpected risk of ePHI are reduced or eliminated. This can be completed by minimizing the exposure of PHI to non-authorized users. For example, if you are working in the SPD department and are asked to go to the critical care floor to deliver a piece of equipment, you would not go behind the nurses station to key in the products identification number to charge the patient for the equipment delivered. As a SPD team member, your access to patient’s PHI would be minimized. Physical safeguards are utilized to secure workstations and other areas in which ePHI may be exposed by enforcing strict policies and procedures to limit this unnecessary exposure to ePHI. Technical safeguards can be used to enforce policies and procedures that prohibit the alteration or destruction of ePHI amongst other measures. These are just a few examples in which Administrative, Physical, and Technical safeguards are used. It is imperative that all staff, regardless of their working capacity/title are educated on compliance with HIPPA that limits excessive and unnecessary exposure to PHI.

Am I in compliance?

As stated previously, Dr. Talk-A-Lot was noncompliant with HIPAA standards by releasing protected health information of his patient Ted. Can you think of a moment in which you may have been out of compliance? Have you discussed an operation that your mother is having with one of your colleagues in the SPD department? Have you tried to research your own medical records at working thinking that it was okay because it’s your record? Have you discussed the prion contamination of your neurological instrumentation received from OR 7 to a friend or colleague at lunch or in the elevator? If so, you are unfortunately, talking too much, and are not incompliance with HIPAA.
As a healthcare worker, yes, even in the sterile processing department you are required to maintain patient confidentiality. Why do we become non-compliant? Is it to be mean, or just plain ruthless? Maybe it’s because of ignorance. HIPAA violations are more common than you may think. According to Zabel (2016), some of the most common reasons medical professionals violate HIPAA occur from the following:

- Gossiping to friends or colleagues in a manner that discloses patient information
- Leaving patient records unsealed in areas where other patients can view them (mishandling patient records)
- Theft or stolen electronic devices such as cell phones, tablets, laptops, etc. that contain PHI and lack safeguards such as password protection and encryption to prevent users from viewing PHI
- Texting PHI to colleagues that can potentially get in the hands of cyber criminals
- Abusing social media sites such as Facebook, Instagram, Twitter, etc. by posting PHI; photos of patients should NEVER be posted onto social media sites.
- Unauthorized employees accessing PHI for whatever reason (spite, nosiness, personal gain, for profit)
- Inquiring about the status of a friend or family member’s medical condition in a public area that exposes their PHI
- Viewing patient records from home or other personal devices that can potentially cause family members of friends to view the PHI
- Lack of or no training regarding how to be in compliance with HIPAA and avoid over-exposure of PHI

If you have found yourself entertaining any of the above-mentioned scenarios, you are most likely not in compliance with HIPAA regulations. It is critical that employers educate their staff to help ensure compliance with these regulations.

What are the consequences for violating HIPAA?

Ensuring compliance with HIPAA is regulated and non-compliance can contribute to fees, fines, termination, and/or jail time. If an institution finds themselves in a situation where they are non-compliant with HIPAA, it is up to that institution to initiate policies and procedures that will get them compliant. If organizations choose to ignore HIPAA regulations they can have civil or criminal charges filed. This year, one of the largest HIPAA settlements in history was recorded when Advocate Health Care failed to conduct extensive risk analysis of its’ facilities that resulted in ePHI being leaked through an unencrypted stolen laptop and four additional stolen computers; this resulted in 4 million individuals being affected and a total fine of $5.5 million (Kohgdai, 2016). According to the American Medical Association (2016) the following penalties are commonly issued to entities or individuals for HIPAA violations:

- Violating HIPAA unknowingly can result in a minimum penalty of $100 per defilement (offense), and a yearly maximum penalty of $25,000 for any repeated offenses. In addition to this, maximum penalties can include a maximum fine of $1.5 million
- Violating HIPAA through reasonable cause can result in a minimum penalty of $1000 per defilement, and a yearly maximum penalty of $100,000 for repeated offenses. In addition to this, maximum penalties can include a maximum fine of $1.5 million
- Violating HIPAA regulations by willful neglect and correcting the violation within the outlined timeframe can result in a minimum violation of $10,000 per defilement, and a yearly maximum penalty of $250,000 for repeated offenses. In addition to
this, maximum penalties can include a maximum fine of $1.5 million

Violating HIPAA regulations by willful neglect and not correcting the violation within the outlined timeframe can result in a minimum violation of $50,000 per defilement, and a yearly maximum penalty of $1.5 million

Prison sentences for HIPAA violations can vary from 1 to 10 years of imprisonment with the addition of fines.

**How do I stay in Compliance?**

Now that you have all of the information that examines how untrained, irresponsible, curious, or spiteful employees violate HIPAA regulations and leak PHI, hopefully, you will refrain from these elements that can leave you with empty pockets and time served! To stay in compliance, follow the rules! Managers and directors should strive to educate personnel on HIPAA regulations. Quarterly or annual training may serve as beneficial to stay in compliance with HIPAA laws. Here are a few other tips that can help you stay in compliance according to Wang (2013):

- Safeguards should be established to protect PHI
- The sharing and usage of PHI should be minimized and retrieved only when absolutely necessary
- Ensure that service providers have Business Associates agreements in place to safeguard PHI effectively
- Initiate training programs to educate employees on effective methods to protect and secure PHI

In closing, it is everyone’s responsibility to ensure that they are compliant with HIPAA. Maintaining the privacy of patients should be a significant concern of all health professionals regardless of the capacity. There are several credible resources available that can help you stay in compliance. Watch what you say. Watch what you do. Be careful of what you see. If it feels like it is an invasion in privacy, there is a high percentage that it is. Be cautious, and make sure that your mouth is HIPAA compliant!

**References**


**What Did I Say? Is my mouth HIPAA Compliant?**

**Post-Test 2016**

1. The acronym PHI stands for public health information.
   - TRUE
   - FALSE

2. Demographic information is not part of PHI.
   - TRUE
   - FALSE

3. Messages and email are the only forms of ePHI.
   - TRUE
   - FALSE

4. HIPAA was founded in 1996.
   - TRUE
   - FALSE

5. Under the Privacy Rule, patients have the right to request a report for why their medical records were shared.
   - TRUE
   - FALSE

6. Ensuring that data stored or transmitted in healthcare is secure is a principle of the Security Rule.
   - TRUE
   - FALSE

7. Physical and Technical safeguards are the only safeguards established under the Security Rule.
   - TRUE
   - FALSE

8. It is okay to leave a patient’s medical record open on the computer screen at work, unsecured if only for a few minutes while I take a bathroom break.
   - TRUE
   - FALSE

9. It is acceptable to text images of a patient having surgery to mother if it’s my brother having surgery.
   - TRUE
   - FALSE

10. Maximum penalties for violating HIPAA regulations can include a maximum fine of $1.5 million.
    - TRUE
    - FALSE

To receive one CEU credit, complete the quiz and send this page only, via normal mail:

Lana Haecherl  
P. O. Box 568  
Pineville, NC  28134-0568

Your certificate will be sent via email if your score is greater than 70%. If you are not a member of NCAHCSP, please include a fee of $20.00 along with your Membership Application, found on the website (www.ncahcsp.org). Please allow at least six weeks for processing.

CEU Expiration Date: November 22, 2021

PRINT NAME CLEARLY: ________________________________

E-MAIL ADDRESS: ____________________________________  □ (New e-mail address)

PHONE NUMBER: ____________________________________
Wally's Seafood Chowder

Wally's Restaurant,
Wrightsville Beach, NC
Servings: 16
Preparation Time: 1 hour 30 minutes

6 Tablespoons butter
1 Cup green onions, chopped
1/2 Cup celery, chopped
1/2 Cup flour
2 Quarts heavy cream
1 Tablespoon chicken stock
1 Pound seafood meat
1 Teaspoon cayenne pepper

Sauté' onions and celery in butter; add flour. (will look like a thin paste)
Heat cream, chicken stock (substitute 1 1/2 bouillon cubes if no stock is available.)
Add sauté' mixture.
Add seafood meat (shrimp, crab meat or imitation crab meat) and cayenne pepper.
Stir constantly at low simmer (DO NOT BOIL!!!) until mixture has reduced down about 1 inch. If too thick add milk.

Per Serving (excluding unknown items): 492 Calories; 48g Fat (86.7% calories from fat); 5g Protein; 12g Carbohydrate; trace Dietary Fiber; 176mg Cholesterol; 285mg Sodium.
Exchanges: 0 Grain(Starch); 0 Vegetable; 1/2 Non-Fat Milk; 9 1/2 Fat.
Dear Steamie,

It seems in the SP profession, it keeps getting more and more challenging. We want to do our best and wanted to know if you may know of some of the areas we need to really focus on?

You are correct. The challenges we face in SP are increasing everyday. There are numerous resources available to help you to ensure compliance. TJC, 3M, ASP and the ECRI Institute made available a list of several Top Risks for SP Departments. Here are the Top 3:

1. Manufacturer's IFU's not being followed. Either the most updated IFU's were not available or were not being followed.
   - OneSource in an excellent web-based resource to ensure you and your department have the most updated info.

2. Insufficient inventory of instruments resulting in IUSS. The Joint Commission and CMS state that IUSS should not be performed due to lack of inventory. Keep diligent records and statistics of all items processed via IUSS. Note any
trends and report these to your Infection Prevention team as well as Surgical Services Leadership to purchase additional items.

3. Improper Processing of Flexible Endoscopes. Cross contamination from flex scopes is one of the most common risks. More often than not the contamination is due to the complexity of the scope itself. Staff training and continuous quality monitoring all assist in proper processing. Don't forget to include in service and remedial training from both your scope reprocessor and scope manufacturer.

Steamie
Future Education Meetings

February 3, 2017 → 2017 NCAHCSP Winter meeting, The meeting will be held in Greensboro, NC at the Northfield Medical Facility.

The annual Spring meeting is April 26 through April 28, 2017, in Myrtle Beach, SC, at the Hilton Myrtle Beach Resort.

Visit our website www.ncahcsp.org You’ll find details as well as brochures and registration information.
Committees for 2016 / 2017

If you are interested in serving on a committee please contact Lana

Education
Angela Chairperson
Stacie
Karen
Katrina
Tammy Brochure

Finance
Frank / Phillip Chairperson
Officers
Board of Directors

Membership
Paul Chairperson
Don
Laura Worley

Editorial
Lana Chairperson
Tammy Dear Steamy
Katrina CEU development

Public Relations
Karen Chairperson
Ann

Recognition
Cheryl Chairperson
Louise
Ann

Nominations
Don Chairperson
Angela

IAHCSMM
Ann Chairperson
Karen
North Carolina Association for Hospital Central Service Professionals will establish itself statewide as the leading educational organization through innovative programs that enhance the development of the Central Service Professionals.
Board of Directors

President — Lana Haecherl  
Manager, Medical Equipment & Sterile Services  
Carolinas Medical Center  
P O Box 32861  
Charlotte, NC 28232  
Phone 704-355-9814  
lana.haecherl@carolinashealthcare.org

Cheryl Bean  
Chief, Sterile Processing  
W.G. ‘Bill’ Hefner VA Medical Center  
1601 Brenner Ave  
Salisbury, NC 28144  
Cheryl.bean@va.gov

Stacie Patterson BSN, RN, CNOR  
RME Coordinator/SPS Nurse Educator  
W.G. (Bill) Hefner VA Medical Center  
1601 Brenner Avenue  
Salisbury, N.C. 28144  
Office 704-638-9000 Ext. 3696  
Stacie.patterson@va.gov

Past President — Ann Thomas  
Instrument Technician IV  
Carolinas Medical Center  
1000 Blythe Boulevard  
Charlotte, NC 28205  
Phone: 704-737-4794  
ann.a.thomas@carolinashealthcare.org

Don Christenbury  
Coordinator, Medical Equipment & Sterile Services  
Carolinas Medical Center  
P O Box 32861  
Charlotte, NC 28232  
Phone 704-355-8924  
Don.christenbury@carolinashealthcare.org

Louise Rahilly, RN  
Founder-Board Member Emeritus  
2623 Fordham Drive  
Fayetteville, NC 28304  
Phone 910-485-8296  
crah115826@aol.com

President Elect — Angela Brockington  
SPD Supervisor  
Duke University Hospital  
2301 Erwin Road, PO Box 100010  
Durham, NC 27710  
Office 919-681-4255  
angela.brockington@duke.edu

Tammy Franklin ST, CSPDT, CSPDM  
Sterile Processing Director  
Catawba Valley Medical Medical Center  
810 Fairgrove Church Rd  
Hickory, NC 28602  
Phone 828-326-3259  
Tfranklin@catawbavalleymc.org

Katrina Simpson, MA CST,CSPDT  
Program Coordinator Sterile Processing  
Fayetteville Technical Community College /  
UNC Medical Center  
PO Box 35236  
Fayetteville, NC 28303  
Phone 910-678-9786  
simpsonk@faytechcc.edu

Treasurer — Frank Sizemore  
Manager, Central Service, Equipment Distri-burion & Material Disposition  
Wake Forest Baptist Medical Center  
Medical Center Medical Center Blvd  
Winston-Salem, NC 27157-1122  
Phone 336-716-6270  
fsizemor@wakehealth.edu

Karen Furr  
Assistant Director Sterile Processing  
Moore Regional Hospital  
PO Box 3000  
Pinehurst, NC 28374  
Phone 910-715-1081  
kfurr@firsthealth.org

Secretary — Paul Hess, BSN, RN, CRCST, ACSP  
Manager, Alternate Site Facilities, Mail Room and Couriers  
New Hanover Regional Medical Center  
2131 S 17th St, P.O. Box 9000  
Wilmington, NC 28402-9000  
Phone 910-343-2142  
Fax 910-343-4400  
paul.hess@nhmmc.org

Phil Hardin  
Supervisor, Sterile Supply Services  
Gaston Memorial Hospital  
Gastonia, NC 28054  
Phone: 704-813-7220

Mailing Address  
NCAHCSN  
605 VALE DRIVE  
WILMINGTON, NC 28411-9484