e-Pursuit

HIM eNews

OrHIMA

AHIMA Affiliate

Oregon Health Information Management Association

# July/

# August 2017

## PRESIDENT'S MESSAGE

**Aurae Beidler, MHA, RHIA, CHC, CHPS,** aurae.beidler@gmail.com
**President**

Welcome to summer! I hope you get out and enjoy the sun and the great outdoors! This time of year it's hard to be inside, stuck in front of a computer. However, we do have some great educational offerings this summer if you can handle being inside. There's always the benefit of air conditioning! The highlight of the summer for coding education is happening on Friday August 11th at the Sheraton Portland Airport Hotel - Spine and Cardiovascular Coding – ICD-10-PCS by national speaker, Lynn Kuehn. We received overwhelming feedback from you after her Fall event that we wanted to bring her back to Oregon. Registration for members is $120 for 7 CEUs!

As we transition our OrHIMA Board, welcoming our newly elected Directors and President-Elect:

- Crystal Clack - President-Elect
- Renee Skeels - Advocacy Director
- Nicole Rodrigues - Public Relations Director
- Janine Gunn - Treasurer
- Stephanie Wirfs - Secretary

I'm excited to see what the new year will hold. We will be continuing the strategic plan that Lynn Edwards and Judi Hoffman have created in past years, but also adding new items and implementing some new initiatives. As I stated at the annual convention, we want to hear from you. What are your ideas? When you think of the HIM profession, where do you want to see it going?

In July, several of the OrHIMA Board members will be traveling to AHIMA's CSA Leadership Symposium to learn more about how to more successfully and effectively guide and lead OrHIMA. We'll be sharing what we learn later this summer.

Please don't hesitate to email me or post a message on the Oregon Engage site. I look forward to hearing from you and helping bring your ideas into action.

Have a wonderful summer and don't forget your sunscreen!

Aurae Beidler, MHA, RHIA, CHC, CHPS
President-Elect

**Professional's Perspective –**


## How to Avoid Common Privacy Notices Mistakes

Most organizations have posted privacy notices on their websites. Great, right? Well consider that a 2012 study showed that the average reader would need 25 days simply to read the privacy policies for all websites accessed in a year. Website privacy notices are often very poorly written. And that's not the only problem, as I've discovered over the past couple of decades reviewing privacy notices. In the past year in the privacy impact assessments (PIAs) I've done, I've found two consistent problems with them all.

- The posted privacy notice for each had not been updated in many years
- No one (literally) within each organization had ever read the privacy notice

I've also found that, generally, most organizations do not understand the purpose of a privacy notice, and are very sloppy in how they post and maintain privacy notice on their web sites, creating significant liability for their organization. Many post a privacy notice once, then never update it again, and others post something to point to for marketing spin to give the impression they care about privacy, but in fact haven't done anything that they've promised.

Here are some privacy notice basics to help organizations better understand how to avoid common privacy notices mistakes.

**Purpose of Privacy Notices**

A posted privacy notice, also often called a "privacy policy" (but I'm going to use the term privacy notice since I typically use policy to reference inward-facing documents for employees to follow) is an outward-facing type of document that is meant specifically for those individuals whose personal information is being collected; the "data subjects."

A posted privacy notice is provided to an organization's data subject audience and should identify:

- The types of personal information items that are collected
- How the personal information is used, retained, disclosed and secured

- The control that the data subjects have over their associated personal information (e.g., specific personal information items that are voluntary to provide, available opt-out options, individual rights of access and correction for associated personal information)

Privacy notices serve two primary purposes:

- Establish accountability for the organization's use, sharing and protection of personal information
- Educate the individuals about whom personal information applies (the data subjects) for their rights regarding their personal information

**Importance of Privacy Notices**

A privacy notice establishes legal accountability for the associated organization to follow the practices that are stated, actually promised, in the privacy notice. Every person within the organization that accesses personal information in some way needs to know, understand and follow the promises made within the privacy notice.

The organization must ensure that every type of computing and digital storage device is configured and used in ways that also support compliance with the privacy notice. This includes all those increasingly used Internet of Things (IoT) devices that are used in ways that involve access to personal information from the organization.

Regulators, auditors, lawyers, and other organizations will judge your privacy program against your organization's practices, and how your managers support them, as they relate to the privacy notice. Here are a few areas where organizations are often violating their own posted privacy notice:

- Lack of accurate details in the privacy notice about the personal information and sensitive information that is being collected, shared, retained and processed
- Lack of information about the purpose(s) for collecting personal information
- A description of the entities to whom, and to which jurisdiction and geographical locations, the personal information might be disclosed or transferred
- How to contact the area responsible for privacy at the organization
- Ensuring that the privacy notice is provided either before or at the time of collection of personal information

**Using Non-Customized Privacy Notices**

Privacy notices must be tailored to the specific data subject audiences. Two common mistakes I've seen organizations, especially those small and mid-size organizations with no position dedicated to privacy and no legal counsel with privacy experience, make is:

- To copy the privacy notice of another organization in their industry and use it verbatim as their own, after simply changing the name of the organization.
- Generating a privacy notice from a free online privacy notice generator and then immediately posting the resulting privacy notice on their website without doing any customization.

It is important to customize privacy notices so that they accurately reflect the organization's collection, use, sharing and safeguards for personal information. The privacy notice is establishing a legal obligation for the organization, so the organization must fulfill those promises. If the organization cannot do what is within their posted privacy notice, then they have created their own legal liability, which could result in significant fines, penalties and civil actions.

**Out of Date Privacy Notice**

Throughout my career I've seen a large portion of organizations that will take action to implement security and privacy practices and then, once done, they forget about it. For example, in my PIAs and audits I've often found organizations who had information security policies that have not been updated in over a decade. I've found this to be true with posted privacy notices as well.

In three PIAs I performed in 2015, I found one had a privacy notice last updated in 2008, one in 2006, and another in 2004. There were references in them to technologies that are not even supported or used anymore, to departments that no longer exist, and phone numbers no longer used; along with other no-longer-valid statements.

Think about how quickly your business changes; in the:

- Types of personal information collected
- Ways in which personal information is used and shared
- Technologies used by all with access to personal information in all forms

When such changes occur, they often will necessitate changes in the posted privacy notice to accurately reflect activities involving personal information. It is important to keep the privacy notice updated and provide an accurate reflection of current practices.

**Personnel Not Knowing What the Privacy Notice Says**

One of the questions I always ask key stakeholders when doing a PIA is, "Have you ever read your web site's posted privacy notice?" In around 95 – 99 percent of the time, no one has even read the posted privacy notice. Ever. These are people who are responsible for personnel, including those who access personal information in some way.

If you have not read the privacy notice, how can you even claim to be supporting the promises made within it for how personal information is collected, used, shared, and safeguarded? You cannot.

To be able to comply with your own privacy notice, you must actually read, understand, and do business in accordance with the privacy notice promises. Your work activities must support the promises.

**Maintain the Privacy Notice**

When it comes to privacy notices, be sure to update them appropriately. Some actions you can take to accomplish this:

- Perform a privacy impact assessment (PIA) for your posted privacy notice to see where you are not in compliance with it, and to determine where changes and updates to the privacy notice are necessary.
- Assign a position or team the responsibility to review the privacy notice at least once a year, and following major operations and technology changes, and to update the privacy notice appropriately.
- Ask legal counsel to monitor changes in data protection legal requirements, and notify the assigned team of such changes so they can be considered when determining how to update the privacy notice.

**Source: Rebecca Herold, Founder, The Privacy Professor®, privacyprofessor.org, privacyguidance.com, SIMBUS360.com, rebeccaherold@rebeccaherold.com**

## Bill Watching in Oregon – 2017 Session

**Laurie Miller, RHIT, CCS-P**
**Advocacy Director**

**For a full description of legislation we are following, please see our March 2017 newsletter or follow the link for details.**

Senate Bill (SB) 860 Relating to mental health treatment providers: The bill processed timely and has been recommended for passing by the Joint Committee on Ways and Means. An amendment directs the Department of Consumer and Business Services to issue a

contract to audit 12 carriers for mental health parity and adequacy of network. Cost of the audits will be the responsibility of the carrier.

SB 397 Directs the Department of Human Services (DHS) to convene a work group to develop a common client confidentiality release form for confidential information sharing between public bodies which include mental health treatment and substance abuse. This bill has appeared to stall in the Senate Committee on Human Services. Fiscal impact has been identified at greater than $150,000 between the various departments slated to be in the workgroup.

SB 275 This bill, if passed, will revise ORS 192-576 regarding providing one free copy of private health information for the purpose of appealing a Social Security Disability denial. A tremendous amount of testimony was presented to the House Committee on Health Care on May 8, 2017. Presenting that day were our friends at DBS Health Information, Oregon Medical Association, Disability Rights of Oregon and two law firms. At this point language changes were offered and support of the bill was near unanimous among those present.

SB 816 This bill permits the Oregon Health Authority (OHA) to require hospitals to submit emergency department (ED) abstract records, in addition to ambulatory surgery and inpatient discharge abstract records. This bill was assigned to the Senate Committee on Health Care in mid-March 2017 after testimony form the Oregon Health Authority (OHA). The OHA sites 1.4 million visits to EDs to Oregon hospitals in 2015. Data collected could be analyzed to assess non-emergency care utilization, psychiatric and behavioral health treatment in ED, public health problems such as opioid overdose, trauma, and appropriate chronic disease management.

Finally, just a word of thank you for your support during my Advocacy Director journey. I'm very proud to have represented OrHIMA and you as members and hope you found my contributions and leadership helpful in your HIM careers. I look forward to transitioning your new Advocacy Director, Renee Skeels, RHIT, CHC.

However, you are not rid of me. I have accepted the position as the HIM Awareness Coordinator for OrHIMA. The HIM campaign has been prepared by AHIMA to help promote the HIM Profession within our industry. Please contact me for more information.

All the best,

Laurie Miller, RHIT, CCS-P

## Spine and Cardiovascular Coding – ICD-10-PCS

## August 11, 2017
## 8:30 AM - 4:30 PM PT

Join us for the Spine and Cardiovascular Coding Meeting on August 11th. This program provides a basic review of both spinal and cardiovascular coding and then helps the attendee through intermediate and advanced discussion of each topic. As always, questions are answered throughout the day. Please see full day agenda.

We will use the 2018 ICD-10-PCS data files from CMS on your laptop or tablet to code cases from the study workbook. Please remember to bring your laptop (or tablet) with the power cord to be able to full participate in the workshop. Bring your printed handout to the workshop if you prefer to write notes on the case. Breakfast and lunch is included in the registration price. The meeting is eligible for 7 CE hours.

***Speaker***

**Lynn Kuehn, MS, RHIA, CCS-P, FAHIMA**
**President, Kuehn Consulting**

Lynn Kuehn is a health care consultant with more than thirty years of experience in the industry. Ms. Kuehn has authored numerous publications for AHIMA including ICD-10-PCS: An Applied Approach 2016 and Procedural Coding and Reimbursement for Physician Services, 15th Edition. She has served as faculty for the AHIMA Train-The-Trainer Academies for ICD-10-CM/PCS Coding since 2010 and was the developer of the ICD-10-PCS Advanced Skills Workshops presented in partnership with AHIMA.

Ms. Kuehn holds a Master of Science degree in Health Services Administration from Cardinal Stritch University and a Bachelor of Science degree in Health Information Administration from Viterbo University. She is a Registered Health Information Administrator (RHIA), a Certified Coding Specialist for Physicians (CCS-P), and a Fellow of the American Health Information Management Association.

***Location***

**Sheraton Portland Airport Hotel**
8235 NE Airport Way
Portland, OR 97220

***Price***

**Early Bird registration ends July 15, 2017**
Members: $120
Non-Members: $140

**Regular registration July 16 – August 7, 2017**
Members: $130
Non-Members: $150

Registration will close at 11:59 PM PT **August 7, 2017.**

Click here to register.

---

**Can Covered Entities Send Unencrypted Email to Individuals? – Comments from HHS**

**Chris Apgar, CISSP, capgar@apgarandassoc.com**
**Director of Communications**

There continues to be confusion about whether or not covered entities and business associates can send PHI to patients using unencrypted email. The answer is yes as long as the patient has been warned about the risks of sending the PHI unencrypted across the Internet and the patient would still like his or her PHI sent via unencrypted email. The following is from HHS/OCR

**Preamble to the Omnibus Rule of 2013**

**Federal Register / Vol. 78, No. 17 / Friday, January 25, 2013 / Page 5634**

Comment: Several commenters specifically commented on the option to provide electronic protected health information via unencrypted email. Covered entities requested clarification that they are permitted to send individuals unencrypted emails if they have advised the individual of the risk, and the individual still prefers the unencrypted email. Some felt that the "duty to warn" individuals of risks associated with unencrypted email would be unduly burdensome on covered entities. Covered entities also requested clarification that they would not be responsible for breach notification in the event that unauthorized access of protected health information occurred as a result of sending an unencrypted email based on an individual's request. Finally, one commenter emphasized the importance that individuals are allowed to decide if they want to receive

Response: We clarify that ***covered entities are permitted to send individuals unencrypted emails if they have advised the individual of the risk, and the individual still prefers the unencrypted email.*** We disagree that the "duty to warn" individuals of risks associated with unencrypted email would be unduly burdensome on covered entities and believe this is a necessary step in protecting the protected health

information. We do not expect covered entities to educate individuals about encryption technology and the information security. Rather, ***we merely expect the covered entity to notify the individual that there may be some level of risk that the information in the email could be read by a third party. If individuals are notified of the risks and still prefer unencrypted email, the individual has the right to receive protected health information in that way, and covered entities are not responsible for unauthorized access of protected health information while in transmission to the individual based on the individual's request.*** Further, covered entities are not responsible for safeguarding information once delivered to the individual. (Emphasis Added)

Template Model Encryption Risk Disclaimer

Sending unencrypted protected health information (your personal health information) over the Internet may result in interception by unauthorized third parties and represents a risk to your privacy. Please acknowledge that you understand and accept the risks related to sending your protected health information (your personal health information) unencrypted over the Internet to [*Provider Name or "to your health care provider"*].

---

## Share Your Ideas –

If you have ideas for articles or email blasts, please submit your ideas to me at capgar@apgarandassoc.com. My goal this year is to send out an email blast weekly to keep you informed and to share ideas that are of importance to HIM professionals. Don't let the thought of composing an article or blast deter you from submitting what you think your colleagues would like to hear. There are no length requirements so it can be as short as you see fit to write.

---

## OrHIMA 75th Annual Conference – Another Great Success

**Dott Campo, RHIT**
**Director of Education**

Whew!! We did it! We planned, set up, ran and attended a pretty darned successful annual convention. Not any old annual convention either – the 75th Annual Convention! It took a lot of hard work from the board and all of our volunteers. Without all of them helping behind the scenes, and you all attending, we would not have had the event we did. We had three days full of amazing speakers and topics. As always, we encouraged all of you to explore the different topics and expand your knowledge. We also encouraged all of you to schmooze and network with those you may not know or even catch up with those you only see yearly at the convention.

I saw these things and more. I am always impressed by our members. Your willingness to learn and grow shines through each and every time. Also, each and every time I am informed by at least a few of our speakers how impressed **THEY** are with our group. We are the *"friendliest and most engaged association"* by far. Thank you!!! Don't forget to fill out the evaluation that KnowledgeConnex sent out. Not only does your completing these evaluations help us in planning next events, once filled out you will be able to download your CE certificate.

Now that annual is over and done with for another year, we are on to planning more events. A couple of events available are:

- **AHIMA Standards and Ethics with Gloryanne Bryant**
  - This is an on demand, free webinar for all of our members.
- **Spine and Cardiovascular Coding in ICD-10-PCS with Lynn Keuhn**
  - This event is a one day, all day, in person event. It is being held at the Sheraton Airport Hotel.

You can find information regarding and links to these events on our website, www.orhima.org.

As I look back on my first year as Director of Education I see all the great events that were put on. My first "official" event, Fall Institute, all the online webinars/education and annual convention. What I see when I look back is not only all the hard work, tears, and time that went into all of them, but also all of the people that helped me accomplish all of it. This is definitely not a one person job. The list of volunteers is mighty as are they and grows daily it seems. The board members, the education committee, the concierges/liaisons, the historical display committee, and just anyone who emailed me with ideas or offers of help. I could not have done it without any of you. Thank you and I look forward to working with all of you and many more in the year to come.

Dott Campo

"Conventioneer Extraordinaire"

## Job Board

- Remote Outpatient Coding Specialist – Health Information Associates
- HIM Coding Supervisor – St. Charles Medical Center
- Remote Inpatient Coding Specialist – Reimbursement Management Consultants, Inc.
- Coding Specialist – Inpatient – Baptist Health South Florida
- Medical Coder – Inpatient – himagine Solutions inc.
- Billing Specialist II – Mid-Columbia Medical Center

To keep up on current postings, check out http://www.orhima.org/him-careers/job-board.


# Be Your Organization's Breakout Star!

## Bring Back Valuable Strategies and Ideas from AHIMA17

The AHIMA Convention and Exhibit is the health information event of the year, bringing together close to 4,500 healthcare leaders, professionals, and stakeholders to address current and emerging industry trends and topics.

There are countless opportunities for you to learn through educational sessions from expert speakers, network with peers from around the globe, and talk with vendors from the industry about cutting-edge solutions and technology in the exhibit hall. All of which offer valuable information that can be taken back to your organization and applied immediately!

### THOUGHT-PROVOKING EDUCATIONAL SESSIONS COVERING...

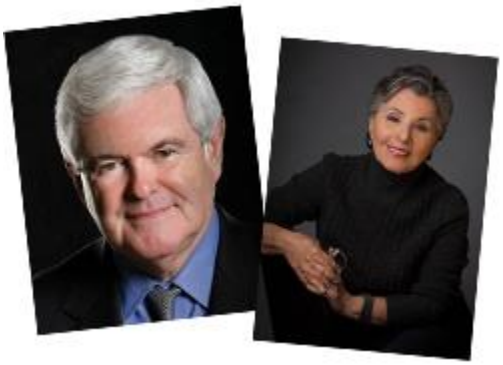
| | |
|---|---|
| Audits | Innovation |
| Clinical Documentation Improvement (CDI) | International |
| Coding | Leadership |
| Consumer Engagement | Payment Reform |

| | |
|---|---|
| Data Analytics | Physician Practice |
| Executive | Population Health/Data Analytics |
| HIM Practice Standards | Post-Acute Care/LTC |
| HIT Standards | Privacy and Security |
| Hot Topics | Quality Measures |
| Informatics | Revenue Cycle |
| Information Governance (IG) | Workforce Development |

Get a sneak peak at this years' sessions with our Convention Planner!

## GENERAL SESSION SPEAKERS INCLUDING...

Point/Counterpoint Session on Healthcare featuring:



**Newt Gingrich**, Former Speaker of the US House of Representatives

**Barbara Boxer**, Former US Senator

An inspiring closing keynote by award-winning actress, **Viola Davis**

Register before **August 21,** to take advantage of early bird savings.

REGISTER

BOOK HOUSING


## CMS – ANNOUNCING NEW STREAMLINED CONTENT

We are pleased to announce the launch of our newly updated Administrative Simplification website—your go-to source for official information from CMS!

Available at a new URL, http://go.cms.gov/AdminSimp, the website features:

- Easier navigation
- Updated and streamlined content

Topics include:

- Electronic transactions
- Code sets

- Operating rules
- Unique identifiers
- Compliance and enforcement

Please note that any bookmarks you have to Administrative Simplification web pages will need to be updated.

Check back often for new information and resources.

**Keep Up to Date!**

- Sign up for Administrative Simplification Email Updates
- Follow us on Twitter

## Have You Looked at Your Medical Record Lately?

**Chris Apgar, CISSP**
**Director of Communications**

We all know patients have the right to request a copy of their designated record set but have you asked for a copy of your own medical record recently? Patient portals are wonderful things. They help us keep track of our medical inforamiton, pick up on new wellness ideas and communicate with our providers. The downside to a patient portal is it usually does not give you visibility into your whole medical record.


As we encourage patients to become more involved in their own care, it's important that we do the same thing ourselves. A glimpse at your full medical record can alert you to inforamtion that may have been added by other providers, provide personal education as to what is included in your record and may serve as a alert to incorrect inforamtion that may be used by your porvider and others for your care.

I periodically request a copy of my medical record to satisify my owne paranoia about someone getting something wrong in additon to make sure I am aware of things like chart notes that may be of importance to me. Yes, I've even found errors such as personal therapy records that identified the wrong body part (my right knee instead of my left knee). I also puruse the patient portal because of the valuable resources it offers. When you request your medical record, remember to make sure you get a complete picture. If you're seeing multiple providers with different EHRs, it's a good ideat to request a copy of your record from all of your providers if your providers are working for different practices and/or hospitals.

Here's to wellness – you all deserve it!

# HHS Office for Civil Rights in Action

## June 30, 2017

## File Sharing and Cloud Computing: What to Consider?

The implementation of file sharing and collaboration tools, including tools that leverage cloud technology, brings with it additional security concerns that HIPAA covered entities and business associates must take into account in their risk analyses, risk management policies, and business associate agreements (BAAs). Cloud computing and file sharing services can introduce additional risks to the privacy and security of electronic protected health information (ePHI) that organizations must identify as part of their risk analysis process and mitigate as part of their risk management process.

For example, a recent survey regarding file sharing and collaboration tools used by organizations from a variety of industries including the healthcare industry, found that just under half of the surveyed organizations stated that they had at least one confirmed file sharing data breach in the last two years.[1] Respondents of this survey listed as their top security concerns: temporary workers, contractors, or third parties accessing data they should not see; employees accidentally exposing data; and broken security management processes.[2] Only twenty-eight percent of respondents listed external hackers as one of their top three concerns.[3]

Additionally, misconfigurations of file sharing and collaboration tools, as well as cloud computing services, are common issues that can result in the disclosure of sensitive data, including ePHI. Too often, access, authentication, encryption and other security controls are either disabled or left with default settings, which can lead to unauthorized access to or disclosure of that data.

Many of these misconfigurations and errors should be detected and corrected as part of an organization's risk analysis and risk management processes or as a result of its evaluation process in response to

[1] Ponemon/Metalogix, *Handle with Care: Protecting Sensitive Data in Microsoft SharePoint, Collaboration Tools and File Share Applications*, https://pages.metalogix.com/ebook-sensitive-data-sharepoint.html, 1.
[2] *Id*. at 4.
[3] *Id*.

environmental or operational changes within the organization. As part of that process, vulnerability scans may help to identify technical vulnerabilities such as missing patches, obsolete software, and misconfigurations of many common file sharing and collaboration tools.

These security concerns are not unique to any particular file sharing or cloud computing technology. Thus, when using these technologies, covered entities and business associates must conduct an accurate and thorough risk analysis, adopt risk management policies to ensure risks are reduced to a reasonable and appropriate level, and enter into comprehensive BAAs (and SLAs where appropriate) to ensure the protection of ePHI and compliance with the HIPAA Rules before implementing any file sharing or cloud computing service that will be creating, receiving, maintaining, or transmitting ePHI.

**OCR Cloud Computing Guidance**

The U.S. Department of Health and Human Services, Office for Civil Rights (OCR) issued guidance in October 2016 to assist covered entities and business associates that decide to utilize cloud computing services how they can leverage cloud technologies while complying with the HIPAA Privacy, Security and Breach Notification Rules (the HIPAA Rules) protecting the privacy and security of ePHI. This guidance addresses key issues, including:

- A cloud service provider (CSP) is a business associate when a covered entity or business associate engages the services of the CSP to create, receive, maintain, or transmit ePHI (such as to process and/or store ePHI) on its behalf.
- The CSP lacking an encryption key to the ePHI does not exempt the CSP from business associate status and its obligations under the HIPAA Rules.
- A HIPAA-compliant BAA is required between the covered entity (or business associate) and the CSP.
- OCR does not endorse, certify, or recommend specific technology or products.
- In addition to a BAA, a Service Level Agreement (SLA) is commonly used to address more specific business expectations between the CSP and its customer (the covered entity or business associate). SLAs, consistent with the BAA, may address HIPAA concerns such as:
    - System availability and reliability;
    - Back-up and data recovery;
    - Manner in which data will be returned to the customer after service termination;
    - Security responsibility; and
    - Use, retention and disclosure limitations.

These are only some highlights from the guidance, which contains eleven key questions and detailed answers. It is important to note that OCR also does not endorse or otherwise recognize private organizations' "certifications" regarding HIPAA compliance, and covered entities and business associates should ensure their own compliance with the HIPAA Rules.

**Read the full guidance**: https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html.

**For more information on HIPAA and Cloud Computing, see**:

1. OCR's Guidance on HIPAA & Cloud Computing, https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html#_ftnref1
2. SP 800-145, The NIST Definition of Cloud Computing, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
3. NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing, http://www.nist.gov/manuscript-publication-search.cfm?pub_id=909494
4. NIST SP 800-146, Cloud Computing Synopsis and Recommendations, http://www.nist.gov/manuscript-publication-search.cfm?pub_id=911075

A PDF of this newsletter may be found on OCR's website at https://www.hhs.gov/sites/default/files/june-2017-ocr-cyber-newsletter.pdf

OCR's Security Rule guidance materials may be found at https://www.hhs.gov/hipaa/for-professionals/security/guidance/

**A BIG SHOUT OUT TO OUR GOLD SPONSOR**

# Gold