



HIPAA Collaborative of Wisconsin 2019 Spring Conference “Feed Your Need for HIPAA Knowledge” April 26, 2019



PROGRAM SUMMARY:

- 7:30-8:30** Registration & Continental Breakfast
- 8:30-8:45** Welcome & Introductions - HIPAA COW President Holly Schlenvogt
- 8:45-10:00** Keynote - Tom Walsh
- 10:00-10:20** Break - Visit with Exhibitors
- 10:20-11:35** Breakout Sessions Group 1
- 11:35-12:35** Lunch
- 12:35-1:25** Breakout Sessions Group 2
- 1:25-1:35** Transition to Next Session
- 1:35-2:40** Breakout Sessions Group 3
- 2:40-2:55** Break - Visit with Exhibitors
- 2:55-3:45** Breakout Sessions Group 4

HOTEL ROOM RESERVATIONS:

For reservations made by **Friday, April 5th**, the rate for a standard room for Thursday evening is **\$104***.

*Rate is subject to state and local taxes and a \$19.95 nightly resort fee.

A special rate of \$149 is also being offered for Friday.

Make Reservations by **PHONE:**

Call 1(800)867-9453 and state that you are with the HIPAA COW Conference at the Glacier Canyon Lodge.

The reference code is #713441.

EVENT LOCATION:
**Glacier Canyon Conference Center,
Part of the Wilderness Resort**

[WEBSITE](#)

45 Hillman Road,
Wisconsin Dells, WI

Directions:

Take I90/94 to Exit #92 (Hwy 12). Go north on Hwy 12 for 4 blocks. Glacier Canyon is on the right.



Our Spring Conference will Feature:

- Shorter, more topic-focused sessions!
- Convenient online registration with the ability to pay via check or credit card.
- Low registration rates of \$150 for Early Bird (deadline April 5) and \$175 thereafter.
- Very affordable hotel room rate of \$104.
- Free Wi-Fi available in the conference center to download presentations.

Continuing Legal Education (CLE) Credits:

We have applied for Wisconsin CLE credits. Once available, we will update the brochure with the number of approved credits.

Registrations for all HIPAA COW events are taken **ONLINE ONLY!**

Please go to our website
hipaacow.org.

Then, go to the **Events Page** for complete details and to register online.

HIPAA 101 Education Materials:

Our website has materials specifically designed to provide an introduction to HIPAA basics. These materials may be especially beneficial to individuals new to HIPAA. If you have a limited understanding of HIPAA, we recommend you view these prior to attending our conference, as our sessions tend to be more advanced. These materials are available on our website resources page:
<http://hipaacow.org/resources>.

Questions? admin2@hipaacow.org or (651)340-6426

Promotional Support:

Wisconsin Hospital Association (WHA)
&
Wisconsin Health Information Management Association (WHIMA)
We thank them for their support!

Our Commitment to Being Green:

Session handouts will be made available prior to the conference so attendees may download the handouts to their mobile devices or print their own handouts. An email with a link to the handouts will be sent to all registered attendees prior to the event.

Keynote Session: Is the Government Indirectly Responsible for Some of the Breaches in Healthcare?

Is the government inadvertently causing data breaches by having healthcare organizations share patient data and expend resources in the wrong direction? Or, are healthcare organizations using the government as a scapegoat for their own short sightedness?

During this keynote, we'll explore all sides of this issue by delivering opposing views as well as a neutral party view.

At the end of this keynote session, attendees will be able to:

- Describe why someone could think the government was indirectly responsible for breaches
- Explain the efforts the government has taken to ensure patient data is protected
- Identify some ideas for moving forward

Tom Walsh, tw-Security

Tom, CISSP is the Founder and Managing Partner of tw-Security, a nationally recognized healthcare security firm that began in 2003.

Tom is a co-author of four books on healthcare information security. He is frequently a speaker at national conventions and is often quoted in trade journals. Tom Walsh and his business partners assist healthcare organizations throughout the country with their information / cybersecurity programs. Tom has over 27 years of information security experience.

Session 101(Privacy): Risk Assessments-Common Myths and Misunderstandings

Risk management is about understanding, not eliminating all risks. In this session we'll cover methods for assessing, analyzing, controlling and documenting risks. We'll review common myths and misunderstandings surrounding the risk analysis.

At the end of this breakout session, attendees will be able to:

- Explain the differences between a HIPAA assessment and true risk analysis
- Execute the nine basic steps of risk analysis
- Use security checklists for determining controls and vulnerabilities
- Discuss methods of documenting risks and management decisions regarding risks
- Identify common mistakes regarding the risk analysis and risk management processes

Tom Walsh, tw-Security

See bio from previous session.

Session 102(Security Technology): Micro-segmentation

This session will explore the advanced security practice of micro-segmentation for customer critical workloads within their data center environment. Justin will review how by implementing automation and orchestration capabilities within network environment, organizations are able to move from traditional provisioning to a more robust and secure approach to intelligently manage operations. Policy and service catalogue management will also be discussed. Lastly, he will provide some recent examples of how he helped organizations architect micro-segmentation strategies to centrally manage and secure their workloads.

Justin Jongbloedt, PDS Inc.

Justin has an extensive background of more than 16 years as an accomplished IT Security leader with experience in multiple settings. His unique expertise ranges from pre-sales and consulting through architecture and ongoing maintenance. As a Solution Architect leader for PDS, Inc., he participates in the proposal and development in several areas – including customer applications, projects and general operations. Justin has an impressive background across a wide range of relevant technologies. He is a key resource for PDS for Cisco UCS, Nexus, VMware, Commvault and several other key technology areas.

Session 103(EDI):

This session is still in the planning stages. The brochure will be updated once information is received.

Mark your calendar with our upcoming conferences:

2019 Fall Conference
October 11, 2019

Red Lion Hotel Paper Valley, Appleton

Mega Healthcare Conference
January 22-24, 2020

Kalahari Resort, Wisconsin Dells

Session 201(Privacy): De-identification

Learn a proven approach to data anonymization that helps you comply with today's rapidly evolving regulatory environment. You'll walk away with practical examples of responsible data sharing to help your organization:

- Protect its reputation while enabling outcomes such as improved analytics, digital initiatives, marketing based on more 'real' looking data and research initiatives
- Deliver the richest possible data at the lowest possible risk to power analytics and strengthen stakeholder relationships

Given the increased HIPAA enforcement, upcoming California Consumer Privacy Act (CCPA) regulations and General Data Protection Regulation (GDPR) potential fines, attendees will learn how to balance their organizations' needs to safely share data with compliance requirements.

Angie Mohr, Privacy Analytics Inc.

Angie helps healthcare organizations turn data privacy into data potential. She enables Fortune 500 and government clients to deploy transformational data strategies, giving them the opportunity to drive population and business outcomes, while meeting regulatory and privacy obligations. Over the past five years, she's helped clients measure the re-identification risk of protected health information and safely anonymize data to the highest possible standard – while preserving its utility. 3M, GE and Washington Healthcare Authority are among the brands that have benefited from Angie's expertise. She holds an MBA from York University, Toronto.

Session 202(Security Technology): Top 5 Ways the Healthcare Industry Can Secure Office 365

Do you know your Office 365 score? Do you know what the Office 365 security score is? If not, this session is perfect for you. We'll showcase this new Office 365 feature and what it means to you. We'll also address the top five ways you can increase your security score to promote regulatory compliance. At the end of this session you'll leave with a better sense of how to have a better Office 365 security posture and a checklist to get started with your Office 365 security journey.

Objectives:

- Discover new security features in Office 365
- Identify measures to help with HIPAA compliance
- Bring back an Office 365 security checklist to your organization

Ryan Peasley, Wipfli LLP

Ryan is an experienced technology consultant, advocate and technology enabler. He has 15 years of experience working with and planning for technology in regulated industries helping organizations manage, implement and utilize technology to engage constituents and customers and achieve organizational goals. His experience includes all aspects of IT service delivery including scoping, planning, migration, configuration, training, documentation, report writing and user adoption.

Session 203(EDI):

This session is still in the planning stages. The brochure will be updated once information is received.

General Session(Privacy/Security/ Security Technology): A Deep Dive into HICP (Health Industry Cybersecurity Practices)

Learn about mitigating common threats to the healthcare industry through a deep dive of the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients document. This guide (written for small, medium and large sized organizations) posits a voluntary, industry-led approach to mitigating five key cybersecurity threats with 10 cybersecurity practices. The work is being produced by the Cybersecurity Sharing Act of 2015 405d Task Group, co-lead by HHS and the healthcare industry. In this session, we will:

- Describe the public-private partnership model developed between the Healthcare Sector Coordinating Council and the Government Coordinating Council
- List the five cybersecurity threats the industry feels are most critical to manage
- Identify the 10 cybersecurity practices to mitigate these threats and their sub-practices
- Discuss how to prioritize the threats for your organization and subsequently the implementation of practices to mitigate these threats

Erik Decker, University of Chicago Medicine

Erik is the Chief Information Security and Privacy Officer for the University of Chicago Medicine. He is the industry lead for a Department of Health and Human Services (HHS) task group of more than 150 industry experts across the country for implementing the Health Industry Cybersecurity Practices (HICP). He is also a member of the Executive Council of the Health Sector Coordinating Council, a joint public-private partnership group tasked with protecting Critical Infrastructure, as defined under the National Infrastructure Protection Plan. He was also awarded the 2017 Chicago CISO of the Year in October, 2017.

Session 303(EDI):

This session is still in the planning stages. The brochure will be updated once information is received.

Session 401(Privacy): GDParrgh! Data Privacy and Security Beyond HIPAA

This session covers how the data privacy and security regulatory landscape in healthcare is changing and what companies should be doing to respond. The presentation will look at the European Union's General Data Protection Regulation (GDPR), the recently passed California Consumer Privacy Act (CCPA), discuss when and how they apply to Wisconsin's healthcare industry and examine how those laws interplay with HIPAA and Wisconsin privacy laws. We will also discuss common misconceptions and mistakes relating to GDPR and CCPA, recent regulatory guidance about the scope and applicability of GDPR and CCPA and best practices for compliance.

Scott LeBlanc, Godfrey & Kahn, S.C.

Scott is an attorney at Godfrey & Kahn in Milwaukee and a member of the firm's Healthcare and Labor and Employment practice groups. Scott represents a wide range of employers, including health systems, hospitals, physician groups and other healthcare related organizations, with respect to employment law and healthcare regulatory issues. His healthcare practice focuses on advising clients both inside and outside of the healthcare industry on health information privacy issues, including but not limited to data breach mitigation and notification requirements and responding to government investigations.

Justin Webb, Godfrey & Kahn, S.C.

Justin is co-chair of Godfrey & Kahn S.C.'s Data Privacy & Cybersecurity Practice Group. His work includes advising clients on preventing and responding to data breaches, cybersecurity and privacy due diligence in M&A, software and technology agreements and compliance with international and U.S. privacy laws. Justin holds the Certified Information Privacy Professional/US (CIPP/US) certification from the International Association of Privacy Professionals. Before his legal career, Justin was the Information Security Officer for a national university where he was responsible for all aspects of the university's cybersecurity, including intrusion detection and prevention, incident response, forensics and ethical hacking.

Session 402 (Security Technology): Privileged Access Management (PAM) & Identity and Access Management (IAM)

PAM and IAM security offer mission-critical solutions to protect privileged credentials from unauthorized access and misuse. They help assure that when perimeter defenses are breached, privileged account controls will act to limit access to sensitive information and curtail an attacker's ability to circulate unhindered throughout the IT environment.

- Protects against internal and external threats
- Meets HIPAA compliance mandates and industry best practices
- Automates scalable security processes so you are more efficient
- PAM provides appropriate access to privileged accounts, bolsters security, achieves compliance, decreases risk, streamlines administration, extends governance and more
- Privilege safe - Automates, controls and secures the entire process of granting privileged credentials
- Session management - Improves security and achieves compliance by limiting privileged access for administrators, remote vendors and high-risk users to a specific duration

Jim Dziak, Axcel Technology

During his career in technology, Jim has served as a CEO of two technology companies that specialized in Enterprise Security and Cyber Security Threat Management. He has been privileged to present PAM and IAM to Security Chapters including the ISSA Wisconsin Chapter, the InfraGard Wisconsin Chapter and Rural Wisconsin Cooperative Health.

Session 403(EDI):

This session is still in the planning stages. The brochure will be updated once information is received.

Thank you to our 2019 HIPAA COW Sponsors:

GOLD:

Quarles & Brady LLP

**HALL
RENDER**
KILLIAN HEATH & LYMAN

WIPFLI LLP
CPAs and Consultants

 **core**

 **Gillware** TM

SILVER:

**GODFREY
KAHN** S.C.

BRONZE:


HRT
Consulting, LLC
Your trusted compliance partner

von Briesen
von Briesen & Roper, s.c. | Attorneys at Law


Boerner
Consulting
LLC

 **PRIVACY
ANALYTICS**
an IQVIA company

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Established in 2001, HIPAA COW is a non-profit organization open to entities considered to be Covered Entities, Business Associates, and/or Trading Partners under HIPAA, as well as any other organization impacted by HIPAA regulations.

The mission of HIPAA COW is to:

- Assist HIPAA Covered Entities, Business Associates, and other interested parties in implementing HIPAA's Privacy, Security and EDI Standard Transaction provisions, as amended over time.
- Foster public education about HIPAA.
- Facilitate and streamline HIPAA implementation through identification of best practices.
- Reduce duplicate efforts among entities obligated to comply with HIPAA.
- Offer opportunities for partnering and collaborating between entities implementing HIPAA.
- Identify and evaluate new or difficult HIPAA interpretation issues.

Cancellation Policy: HIPAA COW reserves the right to substitute faculty or cancel or reschedule programs due to low enrollment or other unforeseen events. If, for any reason, HIPAA COW must cancel this program, registrants will receive a full refund of the registration fee (or a credit to be used for a future HIPAA COW event). Should you be unable to attend, a refund, less a \$25 processing fee, will be given for cancellations received 72 hours prior to the event. No refund will be given if notice is received less than 72 hours prior (even if weather related). Substitutions can be made anytime before the start of the event.

Vendors featuring HIPAA-related products and services will be on site.