VOLUME 18, ISSUE 1 JULY/AUGUST 2023

NABIP 2023 Gold Certified

COIN

NABIP 2023 Pacesetter Award

COUNTY OF ORANGE INSURANCE NEWS

CYBERSECURITY GUIDANCE

Learn about the latest release from US Department of Labor-EBSA regarding Cybersecurity Guidance for Employer Plan Sponsors and Fiduciaries, including:

✓ Tips for Hiring a Service Provider with Strong Cybersecurity Practices
✓ Online Security Tips
✓ Cybersecurity Best Practices

ALSO IN THIS ISSUE:

✓ Compliance Corner: Legal Updates from Marilyn Monahan, Monahan Law Office
✓ NABIP Annual Convention Coverage
✓ New CAHIP-OC Board Elected
✓ California Legislative Updates
✓ And More!

PROTECTING THE CONSUMER'S FUTURE
ORANGE COUNTY CAHIP
California Agents & Health Insurance Professionals
CALIFORNIA'S BENEFIT SPECIALISTS

Health plans that fit every business.

You may face different business challenges today than you face tomorrow. From traditional copayment plans to plans with cost-sharing arrangements, we'll help you find a solution that fits the needs of your business no matter how they evolve. Learn more at **kp.org/choosebetter.**

Choose Better. Choose Kaiser Permanente.

KAISER PERMANENTE® | Business

TABLE OF CONTENTS

Thank you for being a part of CAHIP-OC!

What's Inside

Mark Your Calendars for CAHIP-OC CE Day!

Tuesday, September 12, 2023, Lake Forest Community Center

9 am –3:30 pm

Making a Difference in People's Lives. One Member at a Time.

Our association is a local chapter of the National Association of Health Underwriters (NAHU). The role of CAHIP-OC is to promote and encourage the association of professionals in the health insurance field for the purpose of educating, promoting effective legislation, sharing information and advocating fair business practices among our members, the industry and the general public.

PRESIDENT'S MESSAGE

By: John Evangelista

Dear CAHIP-OC Members,

It feels like I never left, but here I am, returning for another round as your President. I must say, I am thrilled to address you once again as the President of CAHIP-OC. It is truly an honor to serve as your leader and be part of this esteemed organization. As I step into this role, I want to extend a warm welcome to all our new members and express my heartfelt appreciation to our existing members for their continued support and dedication.

First and foremost, I would like to express my gratitude to Pat Stiffler for her exceptional leadership and commitment over the past year. Under her guidance, CAHIP-OC has achieved remarkable milestones, and I am excited to continue to build on that legacy and grow our organization.

I would also like to extend a warm welcome back to the following Board members who have been instrumental in shaping our organization's success: Dave Benson, Dorothy Cociu, Juan Lopez, Sarah Knapp, David Ethington, John Austin, Maggie Stedt, Adriana Mendieta, Louis Valladares, and, of course, Pat Stiffler. To round out our organization, I want to recognize our compass: CAHIP-OC's Executive Director, Gail James Clarke. Gail, thank you for your guidance and for continuing to point us in the right direction. Board members, your expertise and dedication are invaluable, and I look forward to working with each of you to continue driving CAHIP-OC forward.

Let's also give a warm welcome to our new Board members who are joining us this year. Ciaran Patrick is taking the lead as our VP of Professional Development. He has secured a team of three volunteers to help facilitate his endeavors. Cathy Daugherty will be our VP of the Political Action Committee and will lead our efforts to raise funds for NABIP and CAHIP PAC initiatives. We are fortunate to have such talented individuals join our team, bringing fresh perspectives and ideas to further enhance our organization.

This is a critical time in our industry, and your involvement is more important than ever. We have an incredible team of leaders on our Board, and together, we will tackle the challenges we face head-on. From our educational initiatives to advocacy efforts in Sacramento and Washington D.C., there are numerous opportunities for you to make a meaningful impact.

To kickstart our new Board year, we will be holding our 11th Annual Senior Summit from August 22nd to 24th. Come out to Pechanga Resort Casino to learn about the latest and greatest product solutions for your agency and hear from industry leaders and influencers presenting programs sure to help you tackle today's toughest challenges and strengthen your business. Stay tuned for information on additional events, including **CE Day in September**, where you can earn ***five CE credits in one of two different tracks***. **This is also a must-attend event!**

As we embark on this journey together, let's embrace the opportunities that lie ahead. We are living in a unique post-pandemic time, and CAHIP-OC, with its deep understanding of the complexity of the healthcare landscape, has the power to shape the future of our industry. So, let's seize this chance to make a lasting impact and create a brighter tomorrow.

And now, to end on a fun note, here's a little joke for you: Why did the returning President bring a ladder to their inauguration? Because they were aiming for new heights, of course! ***Let's reach for the stars, fellow CAHIP-OC members!***

Thank you all for your unwavering support and commitment to CAHIP-OC. Together, let's make this year the best one yet!

Warm regards,
John D. Evangelista, LPRT
President, CAHIP-OC

Mark Your Calendars for CE Day 2023!

Two Tracks—1) Group & Compliance; 2) Medicare, Individual, Life & Annuities

Tuesday, September 12, 2023

Lake Forest Community Center

Feature Article:

DOL/EBSA Make it Clear That Cybersecurity is a Plan Sponsor and Plan Fiduciary Responsibility

By: Dorothy Cociu, RHU, REBC, GBA, RPA, LPRT
CAHIP-OC VP of Communications & Public Affairs

Ask and you shall receive? Well, although that does not happen as frequently as we'd like, sometimes we are surprised, and it does. In the spring (April) of 2021, the US Department of Labor (DOL) released a much needed (although maybe not wanted by some) guidance package on cybersecurity for plan sponsors and plan fiduciaries. This release didn't get as much press or attention as some releases; perhaps because COVID was still very much a part of our everyday lives at that time. One thing COVID did was bring out more and more bad actors involved with ransomware, malware and other cyber and online threats, perhaps in part because more and more people were working remotely, and where there are remote employees, there is a greater chance of risk and exposure to cyber- attacks. In some cases, examples made national and worldwide news, and affected many of our daily lives. But attacks can and do happen in our offices as well. Keep in mind, where there is data, there is risk of someone gaining access to that data.

Most of us remember the Colonial Pipeline ransomware event in May, 2021. This seemed to be the first of many cyber attacks hitting us that year, but this one really hit home to many. As you'll recall, the Colonial attack is the largest publicly disclosed cyber-attack against critical infrastructure in the United States, attacking the company's IT systems and causing fuel shortages for weeks in the eastern United States. We found out later in news reports that the attack was due to a leaked password, an inactive VPN account and a lack of multifactor authentication. You may also recall that Colonial paid a ransom of millions of dollars to get their systems back up and running. Lucky for them, much of those funds were actually recovered through the tracing of cryptocurrency. Still, the breach could have been avoided if Colonial had used basic cybersecurity practices that experts have been preaching for years. *Could have, would have, should have* been avoided… Yet, these cyber criminals continue to do their damage and far too many companies have been subject to similar circumstances. No one wants to face that moment of shear panic when your systems won't come up, or when they do, and you get a strange and frightening video or screen-shot of someone telling you they now have your data and you must pay to get it back.

The DOL Cybersecurity Guidance was primarily aimed at protecting retirement plans, due to their high financial values and the financial security of so many individuals and families, but the DOL wrote the guidance in such a way to apply to *all* ERISA Plans, including health and welfare plans, because all benefit plans have valuable information (and assets) that cyber criminals want to have their hands on. This has become evident based on the high number of breaches in the health care and health insurance industry in recent years. Remember Anthem, Primera Blue Cross, UCLA Medical Center, New York Presbyterian/Columba Medical Center, Children's Medical Center of Dallas and so many more. ERISA plans not only have financial assets, but personal information that criminals want to exploit. The bottom line is that *the DOL has made it clear that plan sponsors and plan fiduciaries have a responsibility and duty to protect the plan and participants, and therefore have a duty to mitigate cybersecurity risk.*

ERISA and Plan Fiduciary Overview and Background

Before I get into the guidance and how it affects employer plan sponsors and plan fiduciaries, I want to provide a brief background that should help you understand the significance of the role of plan sponsors and their plan fiduciaries in employee benefits.

The Employee Retirement Income Security Act of 1974 (ERISA) includes reporting and disclosure requirements enforced by the Department of Labor (DOL), Employee Benefits Security Administration (EBSA). ERISA is a federal law that regulates employer-sponsored (a) pension plans and (b) employee welfare benefit plans—whether fully insured or self-funded.

Welfare benefit plans include medical, dental, vision, health FSAs, HRA, LTD, STD, life, AD&D, pre-paid legal, some EAPs and some wellness programs.

So, what is a Fiduciary and why is it so important? First off, all ERISA-covered benefit plans are required to have fiduciaries. There are various fiduciary roles under ERISA (both named and functional), including the requirement for each plan to have at least one named fiduciary that must be identified in the plan document (ERISA § 402). The fiduciary is the Plan Administrator (ERISA § 3 (16)). A fiduciary has discretionary authority or control over plan management (ERISA § 3(21)), and a fiduciary is someone who provides investment advice for compensation. Mostly, it's important to note that Fiduciary status is based on the functions performed for the plan, not just a person's title. One thing I always say when discussing the role of fiduciaries, either with an employer client or when teaching a class, is that *If it looks like a duck, walks like a duck, acts like a duck, it's a duck!* Therefore, if you are performing *any* of these tasks, whether or not you've been given the title, you

Continued on page 13

Legislative Updates:

Healthcare Bills in California; Including Single Payer!

By: David Benson - CAHIP-OC VP Legislation

The health insurance industry is very complex. As well intentioned as legislators are when introducing new healthcare legislation, there are always unintended consequences. Your PAC donations get us access to legislators (on both sides of the aisle) whom we can educate on how to eliminate the unintended consequences and still take care of their constituents' healthcare needs.

Some of the bills we are tracking this year include, but are not limited to, expanding health screenings for low-income individuals, keeping provider directories current, expanding the number of languages offered to individuals taking the life or health insurance license exam, balanced billing for ground medical transportation, dental plans would not be able to include pre-existing conditions or waiting periods for dental services and our favorite, a single payer healthcare system. A single sentence "spot bill," AB 1690, was introduced with INTENT language to advance single payer later this legislative session. That bill reads in total: "This bill would state the intent of the Legislature to guarantee accessible, affordable, equitable, and high-quality health care for all Californians through a comprehensive universal single-payer health care program that benefits every resident of the state." This bill is sponsored by the California Nurses Association. This is a 2-year bill. Language will probably be added in January, 2024.

This week a different spot bill, SB 770, was gutted and amended with language that directs *"the Secretary of the California Health and Human Services Agency to pursue waiver discussions with the federal government with the objective of funding a unified health care financing system in California."*

The waivers would redirect all current funding from the Federal Government used for Medi-Cal and Medicare to instead finance single payer creating a government monopoly of medical, behavioral health, pharmaceutical, dental, vision, and long-term care benefits. The current California state budget calls for approximately $235 billion in General Fund spending. The State is projecting a $31 billion shortfall for 2023. State income-tax revenue usually arrives by April 15.th Due to flooding in many of the larger California Counties earlier this year, residents in those Counties do not have to file their income-tax returns until October 15, 2023.

The Office of Management & Budget projected the first-year cost for a Single-Payer Healthcare System to be in excess of $500 billion. In subsequent years, the cost for the Single Payer Healthcare System could increase an average of 5.2%. If California was successful in convincing the federal government to redirect Medicare and Medicaid payments to the Single Payer Healthcare System, that would cover approximately $250 billion of the $500 billion needed to fund the program. Taxes would be raised to cover the remaining costs ($250 billion). *On a humorous note, the California Nurses Association opposes SB 770.*

Over the last few years federal and state legislation passed addressing balanced billing. This is where an insured goes to the emergency room at a network hospital and receives services from an out-of-network emergency room doctor and has to pay the difference in cost between the network and non-network rate. The only service that was excluded from these bills was ground medical transportation. AB 716 (Boerner) addresses this issue. We will keep you updated on the progress of this bill as it works its way through the legislative process.

If you would like to serve on our Legislative Committee this year, please contact David Benson at david@dcbins.com. ##

Congratulations to CAHIP-OC member Meg McComb, who received the California Assembly Resolution for Service in the Community from California Senator Janet Nguyen Spring, 2023

Announcing CAHIP-OC's CE Day 2023!

Tuesday, September 12, 2023

Lake Forest Community Center

9 am—3:30 pm

5 CE Credits Available!

Featuring Two Tracks to Accommodate All Members!

1) Group & Compliance

2) Medicare, Individual, Life & Annuities

Keynote General Session Speaker:
Marilyn Monahan– Monahan Law Office—
Legal Updates for 2023-2024

And Much More!

Mark Your Calendars Now

Outgoing President's Message:

By: Pat Stiffler, Immediate Past President

CAHIP-Orange County had some great events in the past few weeks. At our May meeting the attendees were able to receive the Anti-Fraud Awareness certificate, which is a CA state-mandated CE requirement.

During the awards portion of the meeting, we listed those members with continuous membership for 10 years or more. We also recognized our LPRT and our Triple Crown recipients.

I would like to congratulate our 2022-23 award winners:

Member of the Year	**Legislative Excellence**	**Volunteer of the Year**	**Board Member of the Year**
Cathy Daugherty	Dave Benson	Sue Kidder	Dorothy Cociu

Top Membership Recruiter of the Year
John Evangelista

On June 2, we held our 20th annual Celebration of Women in Business Fashion Show and Luncheon. Since it was our 20th Anniversary and it was also New Hope's 20th Anniversary, we had a Roaring Twenties theme. Many of our guests were decked out in fabulous 20's attire! Our WIB committee did a fabulous job securing amazing raffle baskets and auction items. Macy's provided beautiful clothes and this year our models, and each represented their company in style.

This is my last COIN article as President of CAHIP-OC. It has been my honor and my pleasure to serve as your President. I want to wish John Evangelista, your Incoming President, much success in the coming year. ##

COIN COMPLIANCE CORNER

What Agents and Your Clients Need to Know!

Featuring Legal Briefs By Marilyn Monahan, Monahan Law office and HIPAA Privacy & Security & Related Updates by Dorothy Cociu, CAHIP-OC VP of Communications & Public Affairs

Legal Briefs

This is a summary of some recent developments of interest to consultants and employers—including reminders about some very important deadlines:

FEDERAL: HIGHLIGHTS

Department of Health and Human Services (HHS) Public Health Emergency (PHE): The HHS COVID-19 Public Health Emergency (PHE) ended on **May 11, 2023**. On March 29, 2023, the Departments of Health and Human Services, Labor, and Treasury (the "Departments") issued a set of FAQs—Part 58—to explain the impact of the end of the PHE and the National Emergency (discussed below).

Keep in mind that if you have a fully insured plan, the impact of the end of the PHE could be affected by state law. For example, last year the California legislature passed S.B. 510, and that bill extended coverage for COVID-19 testing, vaccines, and therapeutics for 6 months beyond the end of the PHE. The DMHC and the CDI have issued facts sheets and other resources on this topic:

DMHC: https://www.dmhc.ca.gov/COVID-19.aspx
CDI: https://www.insurance.ca.gov/01-consumers/140-catastrophes/Coronavirus.cfm

Employers and enrollees should check with their carrier for more information on the impact of the end of the PHE on their coverage.

The President's National Emergency (National Emergency): The National Emergency, announced by the president, also ended on **May 11, 2023**. The end of the National Emergency is important because it places an end limit on the mandatory timeframe extensions implemented by the Departments of Labor and Treasury. These timeframe extensions gave participants and beneficiaries extra time to, among other actions, request special enrollment, elect COBRA, pay COBRA premi-

Continued on page 9

HIPAA/HHS/OCR Updates

HHS/OCR have been very busy since the pandemic ended. We are seeing a regular stream of case settlements from the HIPAA Privacy & Security front.

On **June 28, 2023, HHS OCR Settled a HIPAA Investigation with iHealth Solutions Regarding Disclosure of PHI on an Unsecured Server for $75,000.** *iHealth Solutions is a Business Associate and settled a data breach affecting 267 individuals*

HHS and OCR announced a settlement of potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules with iHealth Solutions, LLC (doing business as Advantum Health), a Kentucky-based business associate that provides coding, billing, and onsite information technology services to health care providers. The settlement involved a data breach, where a network server containing the protected health information of 267 individuals was left unsecure on the internet. The HIPAA Privacy, Security, and Breach Notification Rules set the requirements that HIPAA-regulated entities must follow to protect the privacy and security of health information.

"HIPAA business associates must protect the privacy and security of the health information they are entrusted with by HIPAA covered entities," said OCR Director Melanie Fontes Rainer. "Effective cybersecurity includes ensuring that electronic protected health information is secure, and not accessible to just anyone with an internet connection."

In August 2017, OCR initiated an investigation of iHealth Solutions following the receipt of a breach report stating that iHealth Solutions had experienced an unauthorized transfer of protected health information, known as exfiltration, from its unsecured server. The protected health information included patient names, dates of birth, addresses, Social Security numbers, email addresses, diagnoses, treatment information, medical procedures, and medical histories. In addition to the impermissible disclosure of protected health information, OCR's investigation found evidence of the potential failure by iHealth Solutions to have in place an analysis to determine risks and vulnerabilities to electronic protected health information across the organization.

Continued on page 23

ums, and submit claims for benefits. The extra time generally continues until 60 days after the announced end of the National Emergency (this is referred to as the "Outbreak Period"). However, in no event will a person have more than 1 year from the date the action would otherwise have been required or permitted to act. In the Part 58 FAQs, the Departments proposed that if the National Emergency ends on May 11, then the Outbreak Period would end on **July 10, 2023**.

***Prescription Drug Data Collection (RxDC) Reporting*:** The Consolidated Appropriations Act, 2021 (CAA) included a Prescription Drug Data Collection (RxDC) Reporting mandate. Last January, plans and insurers had to file RxDC reports for the 2020 and 2021 calendar years. The 2022 calendar year report was due on **June 1, 2023**. This is an annual reporting requirement—you must report on **June 1** of each year for the prior calendar year—so please mark your calendars accordingly.

Both employer-sponsored group health plans and issuers are independently subject to the mandate and are required to report. Further, the mandate applies whether the group health plan is fully insured or self-funded, whether it is small group or large group, and whether it is grandfathered or non-grandfathered. Church plans and non-federal governmental plans must also report.

If the employer has a self-funded plan, and the employer does not file the data on its own, the employer must contract with one or more third parties—such as a TPA, ASO, or PBM—to file the data on its behalf. If the employer has a fully insured plan, either the carrier will agree to file on the employer's behalf or the employer must do so. If the carrier does not file some or all of the required data—or if the employer did not complete the survey provided by the carrier so that the carrier does not have sufficient data to file all of the required data—the employer remains independently responsible for completing the filing.

***Gag Clause Prohibition and Compliance Attestation*:** Another section of the CAA requires both employer-sponsored group health plans and issuers to remove "gag clauses" from their contracts with any health care provider, network or association of providers, TPA, or other service providers offering access to a network of providers. This mandate to remove gag clauses went into effect **December 27, 2020**—the day the CAA was signed into law.

Both employer-sponsored group health plans and insurers are subject to the mandate. Further, the mandate applies whether the group health plan is fully insured or self-funded, whether it is small group or large group, and whether it is grandfathered or non-grandfathered. Church plans and non-federal governmental plans must also comply.

There is a second part to this mandate: not only must employers and insurers remove gag clauses from their contracts, they must also attest to the Departments that they have done so (the "Gag Clause Prohibition Compliance Attestation"). The first Gag Clause Prohibition Compliance Attestation is due no later than **December 31, 2023**. Subsequent attestations are due by **December 31** of each year, so please mark your calendars accordingly.

On-Line Price Comparison Tool: Both the Transparency in Coverage (TiC) regulations (issued in November 2020) and the CAA require employer-sponsored group health plans and issuers to provide participants with an on-line price comparison tool. This mandate has a staggered implementation process, with the first component going into effect in 2023.

The price comparison tool provides participants and beneficiaries with individually tailored price information for covered items and services. According to CMS, "For the first time, most consumers will be able to get real-time and accurate estimates of their cost-sharing liability for health care items and services from different providers in real time, allowing them to both understand how costs for covered health care items and services are determined by their plan, and also shop and compare health care costs before receiving care."

As a result of the mandate, participants can enter a billing code (or description of a service or item) and a provider name and have the system generate an estimate of their cost-sharing liability for that service with that provider. The cost-sharing estimate will be calculated based on accumulated amounts (for example, how much the participant has already incurred toward their deductible), the in-network rate (including the negotiated rate and the underlying fee schedule rate), and the out-of-network allowed amount.

The price comparison tool must be available for plan years beginning on or after **January 1, 2023**, with respect to 500 shoppable items and services, and for plan or policy years beginning on or after **January 1, 2024,** with respect to all other covered items and services. The 500 shoppable services have already been identified by the Departments implementing the mandate (plans do not get to pick and choose).

***Patient Centered Outcomes Research Institute (PCORI) Fee*:** Self-funded plans must file IRS Form 720, and pay the applicable PCORI fee, each year on **July 31**. The filing deadline is not

Continued on page 10

Legal Updates, Continued from Page 9

based on the plan year—everyone files on July 31.

Form 5500: Do not forget that the Form 5500 must be filed by the last day of the 7th month after the end of the plan year. For calendar year plans, that means that the Form 5500 must be filed by **July 31st**.

***Summary Annual Report (SAR)*:** Do not forget that the Summary Annual Report (SAR) must be distributed by the last day of the 9th month after the end of the plan year (**September 30th** for calendar year plans that did not request an extension of time to file their Form 5500). (In 2023, however, September 30th is a Saturday.)

Preventive Care: A court in Texas, in the *Braidwood Management, Inc. v. Becerra* case, issued an opinion earlier this year that invalidates a portion of the preventive care mandate in the ACA. Under the preventive care mandate, non-grandfathered group health plans must cover preventive services without cost-sharing, so long as the participant receives the preventive service from an in-network provider. Under the court's decision, preventive benefits recommended by the United States Preventive Services Task Force (USPSTF) after the passage of the ACA in 2010 no longer have to be covered. Preventive services recommended by the USPSTF as of the date of passage of the ACA must still be covered, and preventive services recommended by the Advisory Committee on Immunization Practices (ACIP) of the CDC and the Health Resources and Services Administration (HRSA) must still be covered. In addition, plans no longer have to cover PrEP (Preexposure Prophylaxis) therapy, which is used to reduce the risk of HIV transmission, without cost sharing.

To explain the impact of this decision on preventive care benefits under the ACA, the Departments issued FAQs Part 59 on February 23rd. Remember that if you have a fully insured plan, the insurer or HMO will also have to comply with any state rules on preventive care, including those that are more generous than the ACA.

HSA Contribution Limits: The IRS recently announced cost-of-living adjustments for health savings accounts (HSAs) and high deductible health plans (HDHPs) for 2024:

Type of Plan/ Limit		2024	2023
HSA Contribution Limits	Self-Only	$4,150	$3,850
	Family	$8,300	$7,750
HSA Catch-up Contribution	Age 55 or Older	$1,000	$1,000
HDHP Minimum Deductibles	Self-Only	$1,600	$1,500
	Family	$3,200	$3,000
HDHP Maximum Out-of-Pocket Expense Limits	Self-Only	$8,050	$7,500
	Family	$16,100	$15,000
Excepted Benefit HRA		$2,100	$1,950

IRS: Electronic Filing: On February 21, 2023, the IRS issued final regulations on electronic filing requirements. If you will be filing Forms W-2, 1099, or 1094/1095 in 2024, these new regulations impact you.

Under current rules, if you file fewer than 250 of these forms with the IRS, you can file the forms on paper. If you file 250 or more of each, you must file electronically. When calculating the threshold, you look at each type of form separately.

However, for filings made in 2024, the rules are changing. If you file 10 or more of any of these forms—or 10 or more of the forms added together—you must file electronically. For all intents and purposes, this means that all applicable large employers (ALEs) filing the Forms 1094/1095 will have to file electronically in 2024, and many other smaller employers that previously filed certain reports with the IRS on paper will have to make some changes for 2024.

CALIFORNIA: HIGHLIGHTS

In addition to the insurance-related bills CAHIP is tracking, there are (as always) some interesting workplace bills making their way through the state legislature this year. While several of these bills have stalled, they could be taken up again next year, and are therefore worth watching.

***S.B. 73 - Voluntary Veterans' Preference*:** This bill would enact the Voluntary Veterans' Preference Employment Policy Act to authorize a private employer to establish and maintain a written policy to give a voluntary preference for hiring a veteran over another qualified applicant. This bill passed the Senate and is now before the Assembly.

Marilyn Monahan will be our Keynote Speaker in a General Lunch CE Session on Legal Updates at CE Day on September 12, 2023!

Continued on page 12

Top Right: Gail James Clarke, Pat Stiffler, Dorothy Cociu, Shauna Benson at the LPRT Soaring Eagle Pre-Gordon Memorial Reception; Bottom Left: CAHIP President Sue Wakamoto-Lee and her daughter Kylie at the Gordon Memorial dinner.

Follow CAHIP-OC on Social Media!

https://www.facebook.com/OCAHU/

https://www.linkedin.com/groups/4100050/

https://twitter.com/orangecountyahu?lang=en

NABIP Convention - Gordon Memorial Photos

***A.B. 524 - Family Caregiver Status*:** This bill would amend the Fair Employment and Housing Act (FEHA) to prohibit employment discrimination on account of family caregiver status, and would recognize the opportunity to seek, obtain, and hold employment without discrimination because of family caregiver status as a civil right. This bill passed the Assembly and is now before the Senate.

***S.B. 616 - Paid Sick Days*:** This bill would increase the amount of paid sick leave an employer must provide under California's Healthy Workplaces, Healthy Families Act of 2014. This bill passed the Senate and is now before the Assembly.

S.B. 731 - Working from Home: This bill would make it an unlawful employment practice for an employer to fail to provide an employee who is working from home with at least 30 days' advance notice before requiring that employee to return to work in person. The notice must include, at a minimum, prescribed text with information about the rights of an employee to reasonable accommodation for a disability. This bill passed the Senate and is now before the Assembly.

***A.B. 509 - Student Loan Repayment Assistance*:** This bill would conform state tax law to federal law, allowing employers to set up an educational assistance program through which the employer could contribute to the repayment of an employee's student loan debt without tax consequences to the employee. The employer's payment must be made on or after January 1, 2024, and before January 1, 2026. This bill stalled in committee.

S.B. 230 – Health Savings Accounts (HSAs): This bill, for taxable years beginning on or after January 1, 2023, and before January 1, 2028, would allow a deduction in computing adjusted gross income in connection with health savings account contributions in modified conformity with federal law. Once again, an HSA conformity bill failed passage in committee.

***S.B. 703 - Workplace Flexibility*:** This bill would enact the California Workplace Flexibility Act of 2023. The bill would permit an individual nonexempt employee to request an employee-selected flexible work schedule providing for workdays up to 10 hours per day within a 40-hour workweek and would allow the employer to implement this schedule without the obligation to pay overtime compensation for those additional hours in a workday. This bill failed passage in committee.

Civil Rights Department (CRD): Did you know that in July 2022 the Department of Fair Employment and Housing (DFEH) changed its name to the Civil Rights Department (CRD)? The CRD enforces state laws prohibiting hate violence, human trafficking, discrimination in business establishments, and discrimination in government-funded programs and activities, among others. These laws include the Fair Employment and Housing Act (FEHA) and the Unruh Civil Rights Act. The new website is www.calcivilrights.ca.gov. On the website, you will find mandatory workplace posters, guides, and FAQs, among other resources.

MUNICIPALITIES: HIGHLIGHTS

***Minimum Wage*:** Every July 1, a number of municipalities within the state increase their minimum wage. This **July 1**, those municipalities include Alameda, Berkeley, Emeryville, Fremont, City of Los Angeles, County of Los Angeles, Malibu, Milpitas, Pasadena, San Francisco, and Santa Monica. Employers should make corresponding adjustments in their pay structures, update workplace posters, and remember that these increases could impact section 4980H affordability calculations.

San Francisco: Private Sector Military Leave Pay Protection Act ("MLPPA"): A new ordinance took effect in San Francisco on February 19, 2023: The Private Sector Military Leave Pay Protection Act ("MLPPA"). The MLPPA requires covered employers to provide employees with supplemental paid leave for up to 30 days of military duty. The intention is to ensure that an employee will not suffer financial hardship during military duty. The San Francisco Office of Labor Standards Enforcement administers and enforces the MLPPA.

Employers with 100 or more employees worldwide are considered "Covered Employers" and must comply with the MLPPA for their covered San Francisco employees. The City and County of San Francisco and all other governmental entities are not Covered Employers. Employees, including a part-time and temporary employees, who perform work for the employer within the geographic boundaries of San Francisco, are covered by the ordinance if they are a member of the reserve corps of the United States Armed Forces, National Guard, or other uniformed service organization of the United States. ##

Editor's Note: Marilyn Monahan can be reached at marilyn@monahanlawoffice.com

Register Now for Senior Summit, 2023!

See pages 24 &25 for more information!

Feature Article, DOL Cybersecurity Requirements, Continued from Page 5

are, indeed, a fiduciary.

There are four main fiduciary duties under ERISA: 1) the Duty of undivided loyalty to plan participants and beneficiaries (exclusive benefit rule), including acting for the sole purpose of providing benefits to plan participants, which includes the requirement that you must only pay reasonable plan expenses; 2) Duty of prudence (Prudent Man/ Person Standard of Care). ERISA requires that plan fiduciaries must act with the care, skill, prudence, and diligence under the circumstances then prevailing, that any prudent person acting in a like capacity and familiar with such matters would use. What has now been added to these duties is an obligation to ensure "proper mitigation of cybersecurity risks." 3) Duty to diversify assets of the plan; 4) Duty to administer the plan in conformity with governing documents. The DOL understands and encourages plan fiduciaries to get help if and when they need it from experts.

Why Cybersecurity Compliance Matters

For an employer sponsoring an ERISA benefit plan, cybersecurity compliance matters because It's the legal standard, it is part of the Plan Administrator's fiduciary responsibility, it's an employer obligation – not an insurer or broker obligation, it's needed and expected to fix problems, be ready to respond to participant inquiries or complaints, as well as be ready in the event of a lawsuit. In addition, compliance matters so that you're prepared in the event of a DOL, IRS, or HHS/OCR audit, prepared in the event of a merger, or wish to be a hero to the CEO/CFO, and if self-funded, it is required to be complaint with stop loss requirements, to name a few reasons.

Real-World Applications of Cybersecurity Compliance

As I said previously, the DOL released their Cybersecurity Guidance in April, 2021 for plan fiduciaries, plan sponsors, recordkeepers and plan participants. Why have they released them?

Without sufficient protections, "participants and assets may be at risk from both internal and external cybersecurity threats. ERISA requires plan fiduciaries to take appropriate precautions to mitigate these risks." In addition, "This much-needed guidance emphasizes the importance that plan sponsors and fiduciaries must place on combatting cybercrime and gives important tips to participants and beneficiaries on remaining vigilant against emerging cyber threats."

I asked Marilyn Monahan, our Benefits Attorney, if she thinks plan sponsors and plan fiduciaries should be taking this seriously and if so, why? "By issuing this summary of 'best practices,' the DOL has announced that this is an area of concern and focus. Further, in the introductory paragraph of the guidance, the DOL clearly ties these best practices to existing ERISA fiduciary standards: 'Responsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks.' Responsible plan fiduciaries would be well advised to take note."

I asked our technology/IT and cybersecurity partners, Ted Flittner and Ted Mayeshiba of Aditi Group, if they thought plan sponsors and plan fiduciaries should be taking this cybersecurity guidance seriously, and if so, why.

"Dorothy, I have money in a plan. If it goes missing, you can bet I'm coming after my money," stated Ted Mayeshiba, Principal. "Plan fiduciaries are named that [fiduciaries] because there is a responsibility to safeguard MY MONEY. There are too many horror stories which relate fiduciaries having individual accounts under their control hacked and money stolen. Now, with these guidelines, the legal standard of "duty of prudence" have been clarified. Meaning, if you don't follow these guidelines, you are more likely to be on the losing end of a judgement."

His partner Ted Flittner continued: "This is the DOL's way of making Cybersecurity an official, formal and now expected part of doing business in employer/employee related areas. Not following guidance is asking for investigation, judgement against you and penalties. But aside from the "legal" or DOL impact, the guidance offered is just plain SMART and good for everyone."

For another opinion, I spoke with Adriana Mendieta, an industry friend, CAHIP-OC member and fellow cybersecurity business associate, who is a database manager for Colonial Life and also specializes in cyber liability insurance coverage. "Plan sponsors and plan fiduciaries should indeed give serious consideration to the Department of Labor's requirement for Cybersecurity Policies and Programs," stated Adriana. "Cyber threats pose a substantial risk to ERISA plans, and it is crucial for sponsors to prioritize the protection of assets, compliance, and safeguards. In my role, I strongly believe that cyber insurance plays a vital role in ensuring the cybersecurity of the plan."

The guidance "complements EBSA's regulations on electronic records and disclosures to plan participants and beneficiaries. These include provisions on ensuring that electronic recordkeeping systems have reasonable controls, adequate records management practices are in place, and that electronic disclosure systems include measures calculated to protect Personally Identifiable Information."

I asked Marilyn Monahan, if she agreed with me that the release of such guidance means that they are putting a much higher emphasis on cybersecurity in benefit plans. "Yes," Marilyn replied. "In fact, it is clear that cybersecurity is a priority not only with the DOL, but also with other federal agencies and at the state level as well. (The California Consumer Privacy Act of 2018 (CCPA)—as modified by the California Privacy Rights Act (CPRA)—is an example of the increasing interest in cybersecurity at the state level.) While this interest can seem to create significant challenges for employers and producers as they work to understand how multiple—and potentially overlapping—standards apply to them and their benefit plans, taken together they do also send a clear message that cybersecurity is a priority to regulators and must be to employers as well."

The DOL/EBSA Guidance divides the Guidance into three sections, which I will divide by topic for readers. I asked Marilyn to give me her thoughts on why it is important that a plan sponsor or plan fidu-

Continued on page 14

Feature Article, DOL Cybersecurity Requirements, Continued from Page 13

ciary create a complete Cybersecurity Program now. "The guidance was issued in 2021—a couple of years ago," Marilyn stated. "The COVID-19 National Emergency and PHE are now over. With things getting back to 'normal," this is a good time for employers to turn their attention to all aspects of compliance, including cybersecurity."

Tips for Hiring a Service Provider with Strong Cybersecurity Practices

In the first of the 3-part guidance, the DOL focuses on tips for hiring service providers with strong cybersecurity practices. Business owners have a fiduciary responsibility under ERISA to prudently select and monitor service providers. *The guidance makes it clear that each plan sponsor must have a process in place for selecting your service providers.* One question you need to ask them is if their "process" is completely documented? This should be made a part of your RFP process. Then plan sponsors need to find out from the service provider how they monitor their electronic files and data and be sure that every step is completely documented. Plan sponsors/fiduciaries should monitor not only new service providers, but current providers as well.

The service provider or providers should have in place a recognized standard of information security and outside monitoring procedure. Do they have a documented standard of information security that tracks the who, how, why, when for everything they have in their possession? Lastly, plan sponsors should ask who is overseeing the process? Each service provider should assign an individual or team to oversee the process, and the employer/plan sponsor/fiduciary should be asking for details on this procedure (or procedures).

Another step in hiring a service provider with strong cybersecurity practice, according to the DOL Guidance, is to be sure they have in place a vendor/service provider validation of practices, so that you can see their track record, their past security breaches and how they mitigated those breaches. Is there public information regarding security incidents or breaches, other litigation and/or legal proceedings related to the vendor's services? Plan sponsors should ask them what their internal process is for all of these items, and perhaps do some google and other types of public searches as well, and not rely entirely on what the vendor tells them. My motto for this is *trust, but verify!*

Other things plan sponsor/fiduciaries can do is to check the HHS "Wall of Shame" for Large Breaches (those covered under HIPAA Privacy & Security rules are required to report their breaches to HHS/OCR; those with over 500 affected by the breach are posted on their "Wall of Shame" – a term that the industry coined for the website pages on breaches), google newspapers that monitor breaches, and check newspaper articles to see if their name comes up related to breaches that may have been smaller than those posted on Wall of Shame. In addition, they can ask for client references and ask questions about whether they know of any security breaches. What happened? How was it documented and reported? How did the service provider respond overall? How was it mitigated?

We all know that things can happen, no matter how secure you may think you are. After all, we're all dealing with the "weakest link," which is human beings; our employees. That's why it's important to have insurance policies in place to cover losses. Therefore, the Guidance asks if you're verifying if the service provider has cyber liability insurance. In order to be approved for cyber liability coverage, you must have written procedures in place, so having it tells you a lot. You may want to ask them for a copy of their cyber liability policy… If you have that, you can check to see what their policy covers. Will it cover losses caused by cybersecurity and identity theft breaches (including breaches caused by their own internal threats, such as misconduct by the service provider's own employees or contracted vendors, and breaches caused by outside threats, such as a third party hijacking a plan participant's account)?

The Guidance also suggests that plan sponsors have contract terms that actually require certain cybersecurity standards. A plan fiduciary should review their agreements and see if they have added cybersecurity standards to your vendor agreements.

Process for Comparing and Selecting a Service Provider

The first step for a plan sponsor is to look for service providers that follow a recognized standard for information security and use an outside (third-party) auditor to review and validate their cybersecurity practices. They can do this with annual audit reports that verify information security, system/data availability, processing integrity, and data confidentiality.

Next, they will want to know how the service provider validates its practices, and what levels of security standards it has met and implemented. In doing this, they should be sure you have contract provisions that allow the plan sponsor the right to review audit results demonstrating compliance with the standard. They may want to verify that the contract requires ongoing compliance with cybersecurity and information security standards and watch for and beware of contract provisions that limit the service provider's responsibility for IT security breaches. They should have a consultant or attorney review the contract to see if it has or you can add appropriate terms to enhance cybersecurity protection for the Plan and its participants, including information security reporting, clear provisions on the use and sharing of information and confidentiality of information. Does it meet a strong standard of care to protect confidential information against unauthorized access, loss, disclosure, modification or misuse? Does the contract require that they notify the plan sponsor about cybersecurity breaches, and if so, when/how quickly?

Additional contract terms of a Service Provider to look for includes looking to see if they require ongoing cybersecurity and information security standards and compliance. Do their contracts limit the service provider's responsibility for IT security breaches? That could be a reg flag and prompt to check into it further. Plan sponsors should consider including terms that would enhance cybersecurity protection for the Plan and its participants, including (but not limited to): Information Security Reporting – annually obtaining third-party audits to determine compliance with IT P&Ps; Clear Provisions on the Use and Sharing of Information & Confidentiality – spell out service provider's obligation to keep private information private, prevent the use or disclosure of confidential information without written permission, and meet a strong standard of care to protect the confidential information against unauthorized access, loss, disclosure, modification, or misuse.

While plan sponsors are looking at contracts, they should Include terms that would enhance cybersecurity protection for the Plan and its participants, including (but not limited to): Notification of Cybersecurity Breaches – identify how quickly they would be notified of any cyber incident or data breach, and ensure the service provider's cooperation to investigate and reasonably address the cause of the breach; Compliance with Records Retention & Destruction, Privacy & Information Security Laws – specify the service provider's obligations to meet all applicable federal, state and local laws, rules, regulations, directives and other governmental requirements pertaining to the privacy, confidentiality or security of participants' personal information; Insurance - the Plan Sponsor or Fiduciary may want to require insurance coverage such as professional liability, E&O, cyber liability, and privacy breach insurance, and/or fidelity bond/blanket crime coverage.

Cyber insurance in today's world is critical for most, if not all, service providers. "One vital aspect of a well-rounded cybersecurity plan is being prepared for every possible scenario," stated Adriana. "Cyber insurance can play a crucial role in reducing the financial impact of a cyber incident. It offers coverage for various expenses, such as legal and forensic services, breach notification, credit monitoring, public relations, and potential regulatory fines. By obtaining cyber insurance, plan sponsors and fiduciaries can transfer some of the financial risks associated with cyber incidents to an insurance provider, providing an additional layer of protection for plan assets. Furthermore, cyber insurance can provide additional benefits beyond financial protection. Many insurance providers offer proactive risk management services and resources to policyholders, such as cybersecurity training, vulnerability assessments, and incident response support. These services can assist organizations in strengthening their cybersecurity posture and enhancing their overall resilience against cyber threats. However, it is important to acknowledge that cyber insurance should not be viewed as a substitute for a comprehensive cybersecurity plan. It is merely a component of a broader strategy that encompasses preventive measures, employee education, regular system updates, and ongoing monitoring. Having a formal cybersecurity plan in place provides a structured approach to safeguarding critical assets and minimize the potential impact of cyber incidents, including the role of insurance."

The guidance states that when a plan sponsor contracts with a service provider that the plan sponsor/fiduciary makes sure that the contract requires ongoing compliance with cybersecurity and information security standard, and be aware of provisions limiting the service provider's responsibility for IT security breaches. I asked Marilyn, as an attorney, what kind of provisions she would recommend be included in vendor contracts related to these requirements? "If the draft agreement comes from the service provider, do not take the contract terms for granted. Be certain that the contract addresses the issues that are most important to you, and provides you with assurances that security compliance will satisfy designated industry standards, not only as of the date the contract was signed, but on an ongoing basis. The DOL's guidance provides some terms to consider." *Again, trust, but verify!*

A well thought-out fiduciary questionnaire should allow the plan sponsor to compare each service provider based on how they answered their questionnaire. With this, they can then have a committee meeting or meetings to compare and evaluate the submitted questionnaire, document the positives and negatives of each, and place a value or score on each for comparison purposes. After discussions and evaluations, they should make their service provider selection based on the final "value" or "score" of each to justify why this selection was made.

Why is it important to hire service providers with strong cybersecurity practices? "For two key reasons," stated Monahan. "First, because choosing the right service provider is a fiduciary function. (This point was also emphasized by the new CAA compensation disclosure rules.) Second, because loose cybersecurity practices by a service provider create vulnerabilities, and vulnerabilities could result in a breach that could harm the employer and plan participants."

Service Provider Monitoring

The DOL Guidance also requires plan sponsors/fiduciaries to create a cybersecurity service provider monitoring process. Questions plan sponsors should ask include: a) what categories are you monitoring?, b) how often are you monitoring?, c) who is assigned to monitor?, d) do you have a documented process for all of this?

As a Plan Sponsor/Fiduciary, what will your clients do when they see insufficiencies or failures to perform? What is their process in reporting this to the service provider and getting resolution or improvements? Have they looked for who, what, when, and how? Again, the plan sponsor should have all of these processes in place, and the ability to make corrections and changes as needed.

The Guidance makes it clear that a plan sponsor/plan fiduciary has an obligation to be sure that their vendor/servicer providers are using a recognized standard of information security and one or more outside third party auditors to review and validate cybersecurity.

As a plan sponsor/fiduciary, your clients' confidence in a service provider increases if the security of its systems and practices are backed by annual audit reports that verify information security, system/data availability, processing integrity, and data confidentiality.

Other overall tips for Hiring a Service Provider with strong Cybersecu-

Continued on Page 16

Feature Article, DOL Cybersecurity Requirements, Continued from Page 16

rity Practices include of course, checking references, getting a consultant Seal of Approval, and using Legal Counsel when appropriate.

Cybersecurity Program Best Practices

A Formal, Well-Documented Cybersecurity Program

The Guidance calls for a formal, well documented cybersecurity program. According to the DOL, a sound cybersecurity program identifies and assesses internal and external cybersecurity risks that may threaten the confidentiality, integrity or availability of stored nonpublic information. Under the program, the organization fully implements well-documented information security policies, procedures, guidelines and standards to protect the security of the IT infrastructure and data stored on the system.

A "prudently designed" program will protect the infrastructure, information systems and information in the systems from "unauthorized access, use, or other malicious acts by enabling the organization to identify the risks to assets, information and systems; protect each of the necessary assets, data and systems; detect and respond to cybersecurity threats; recover from the event, should one occur; disclose the event as appropriate; restore normal operations and services and quickly and efficiently as possible."

Why is this formal program so important in protecting plan assets and overall ERISA compliance? "There are several good reasons for having a written program," stated Marilyn. "One of those reasons is that the drafting process, on its own, is an important tool that can be used to identify and address both cybersecurity vulnerabilities and corresponding solutions. In addition, a written standard gives you a starting point for compliance, as well as a reference point for ongoing risk analysis and upgrades. Finally, if you are audited, a well-written and well-thought-out program will provide proof of your commitment to cybersecurity."

Should plan sponsors and plan fiduciaries be taking this seriously and if so, why? "By issuing this summary of 'best practices,' the DOL has announced that this is an area of concern and focus," stated Marilyn. "Further, in the introductory paragraph of the guidance, the DOL clearly ties these best practices to existing ERISA fiduciary standards: 'Responsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks.' Responsible plan fiduciaries would be well advised to take note."

A formal, well-documented cybersecurity program should establish strong security policies, procedures, guidelines and standards that meet the following criteria:

- Approval by senior leadership
- Review at least annually with updates as needed
- Terms are effectively explained to users
- Review by an independent third-party auditor who confirms compliance
- Documentation of the particular framework(s) used to assess the security of its systems and practices.

The DOL's best practices guidance states that plan sponsors/fiduciaries should have formal and effective policies and procedures in place that govern things like data governance and classification; access controls and identity management; business continuity and disaster recovery; configuration management; asset management; risk assessment; data disposal; incident response; systems operations; vulnerability and patch management; system, application and network security and monitoring; systems and application development and performance; physical security and environmental controls; data privacy; vendor and third party service provider management; consistent use of multi-factor authentication; cybersecurity awareness training, which is given to all personnel at least annually; encryption to protect all sensitive information being transmitted and at rest.

"It's important to note that cybersecurity is a complex and ever-changing field," stated Adriana. "Striking the right balance between regulation and innovation is crucial. Overly burdensome regulations could stifle innovation and impose significant costs on businesses, particularly small and medium-sized enterprises. Any government efforts to enhance cybersecurity requirements should be carefully crafted, taking much into consideration. It may be beneficial for the government to reassess and potentially enhance their requirements should be done thoughtfully, in collaboration with industry experts, and with a clear understanding of the potential impact on businesses and the overall digital ecosystem. Cyber Insurance providing financial backing should also be considered as a part of the solution."

I asked Aditi Group Principals how important it is to have Senior Leadership involved with the cybersecurity program and why? "The company is at risk," replied Mayeshiba. "Addressing that risk must be made by Senior Leadership. Assigning ultimate responsibility for the various cybersecurity functions must be made so that the POSITION, not the person, is the RIGHT person to take action."

"We also know that actions speak louder than words," commented Flittner. "When we see people at the top involved, we know it's important."

This sentiment was echoed by Adriana Mendieta, cyber liability insurance expert. "Having Senior Leadership engaged in the cybersecurity program is crucial. Leadership sets the tone, allocates resources, makes decisions and are key in incident response and compliance + legal considerations."

Prudent Annual Risk Assessments

Risk assessments are necessary and of the utmost importance. In a risk assessment, you can identify, estimate, and prioritize information system risks. IT and cyber risks are constantly changing, and your risk assessment schedule should reflect that. If the plan sponsor wants to be safe, they must constantly adapt to new threats and know how to mitigate them. Waiting only puts the plan sponsor's firm and their assets, including their data, at greater risk.

Why is this documentation and annual risk assessment so important? "When you're standing in front of a judge, they want to see evidence that you've at least made a good faith effort to comply. This is your vehicle," stated Mayeshiba.

Flittner commented: "Remember the mantra: If it's not in writing, it didn't happen. Assessments, action plans, and notes along the way become the evidence that a program IS real. Investigators look for these documents right off the bat. Every business changes and technology evolves so quickly year after year that what we thought was "safe" last year may not be now. Risk assessment MUST be a repeated action or risk will grow and grow over time.

So what does a Prudent Annual Risk Assessment accomplish? "The environment is constantly changing," stated Mayeshiba. "Cybercriminals are improving their techniques, software and attacks. As we know more, we need to assess differently. It's 'whack-a-mole.'"

"Documentation and annual risk assessments are critical components of a proactive cybersecurity approach," stated Adriana. "They help organizations identify and mitigate risks, ensure compliance with regulations, enable effective incident response, and enhance the prospects of obtaining adequate cyber insurance coverage."

Adriana continued," Prudent Annual Risk Assessment is a vital tool in the world of cyber, particularly when it comes to qualifying for cyber insurance. It enables organizations to identify, quantify, and mitigate risks, and are prepared or not to respond to any cyber incidents."

A Reliable Annual Third-Party Audit of Security Controls

It's vitally important that your plan sponsor clients have an independent auditor assess an organization's security controls which provides a clear, unbiased report of existing risks, vulnerabilities and weaknesses. As I always say in training, an in-house IT Team should NEVER evaluate its own in-house security. It's like putting a proverbial chicken in charge of watching the hen house… or in more corporate terms, an IT Team is stressed enough. If they know that an outside audit could result in them having to do more work, or modify or change what they spent months or longer putting in place, they tend to be a bit protective of their work, and time and energy put into it. Therefore, in their eyes, and in reports to senior management, they are less likely to report their own weaknesses. Sometimes it takes an outside auditor to put the spark under them to make them tighten things up to be more secure.

"Involving an independent third-party in reviewing a cyber program and policies brings objectivity, expertise, credibility, compliance verification, and risk mitigation to the process. Their involvement strengthens the overall effectiveness of the program, instills confidence and helps organizations stay resilient," commented Adriana.

The Best Practices guidance states that the program and policies should be reviewed by an independent third- party auditor who can confirm compliance. I asked Aditi Group why is this third party so important, and is this something that Aditi Group does for employer plan sponsors?

Flittner responded: "The outside viewer can spot things that insiders look past or forget about. And insiders often just assume something has to be a certain way – "it's always been this way." And impartiality allows an outside viewer to highlight and include things that may be too sensitive or political hot potatoes.

"Yes, we have done these audits," confirmed Mayeshiba. "Sometimes, the company comes to us and says, 'we've done our best, can you please review our situation and documentation?' We have also started from scratch with companies that have nothing in place and want us to build something for them." So there is help out there, if you need it.

Clearly Defined and Assigned Information Security Roles and Responsibilities

The DOL Guidance clearly states that for a cybersecurity program to be effective, it must be managed at the senior executive (fiduciary) level and be executed by qualified personnel. The Guidance calls for the Chief Information Security Officer (CISO) to establish and maintain the vision, strategy, and operation of the cybersecurity program which is performed by qualified personnel who should have sufficient experience and the necessary certifications; the program should be subject to initial and periodic background checks (because, let's face it, things happen since people were hired); the program should include regular updates and training to address current cybersecurity risks; the program should reflect current knowledge of changing cybersecurity threats and countermeasures.

Strong Access Control Procedures

Access control, says ABC, Aditi Group and the DOL, is a method guaranteeing that users are who they say they are and that they have the appropriate access to the systems and data. This includes two main components: authentication and authorization. The Guidance provides best security practices for access control, which again, is consistent with those provided by ABC and Aditi Group. They include access to systems limited to authorized users, process, devices, activities and transactions; access privileges, which are reviewed at least quarterly; a requirement for complex and unique passwords; multifactor authentication; P&Ps and controls to monitor activity and detect unauthorized access, use of or tampering with nonpublic information; procedures that ensure sensitive data about a participant or beneficiary in the service provider's records matches the information that the plan maintains; confirmation of identity of the authorized recipient of any funds.

Assets or Data Stored in a Cloud or Managed by a Third-Party Service Provider Subject to Appropriate Security Reviews and Independent

Continued on Page 18

Feature Article, DOL Cybersecurity Requirements, Continued from Page 17

Security Assessments

Cloud computing always has dangers and challenges. A cloud means that a third-party is storing the data. Organizations must understand the security posture of the cloud service provider in order to make sound decisions on their services. Best practices include requiring a risk assessment of third-party service providers; defining minimum cybersecurity practices; periodically assessing third party providers based on potential risks; and ensuring that guidelines and contractual provisions protect all parties. Agents and their employer plan sponsors should be sure to have a HIPAA Business Associates Agreement in place with all cloud providers if there is any HIPAA or related information stored there.

Why is it best to have a third-party cloud provider reviewed and have independent security assessments? "The "Cloud" is too easily out of sight and out of mind," commented Flittner. "It's too easy to ignore risks that can be understood and addressed. Sometimes an assessment leads us to make big changes. And change can mean more work for someone for a time. It's easier to not look and pretend that it's all ok…" Mayeshiba commented: "Cloud computing has become very powerful and ubiquitous in the business. Everywhere your data resides, every link from your business to that data, is at risk. Do you have an agreement in place with your cloud provider that insures your data from breach? Probably not. No one can realistically take that bet, because you (the user) may well be culpable for the data breach on their cloud system. So could others in the supply chain. Yes, a security assessment should be done on all 'third party vendors' including cloud providers."

"When an organization entrusts its data to a cloud provider or a third-party service, it essentially transfers some level of control and responsibility for the security of that data," Adriana commented. "Then it becomes essential to thoroughly review and assess the security measures implemented by these providers to the same accountability of other 3rd party providers."

Cybersecurity Awareness Training Conducted At Least Annually

As we've been saying at ABC and Aditi for over a decade, the weakest link of any organization's cybersecurity is their own employees. How well or how little you and your clients train them will determine their fate in most cases. It's imperative that all plan sponsors and their vendors train their employees at all levels of the risks, what to look for, and what to do and not to do (such as clicking on links that may result in malware, ransomware or other cyber threats entering your systems). I'm happy that finally the federal government has put a priority on training and is stating that it should be done at least annually. Without prior guidance, some firms went years before re-training their staff.

Secure System Development Life Cycle Program

The DOL's Guidance recommends a secure SDLC process that ensures that security assurance activities such as penetration testing, code review, and architectural analysis are an integral part of the system development effort. This includes such protections as configuring system alerts to trigger when an individual's account information has been changed; requiring additional validation for distributions; requiring additional validation if personal information has been changed prior to a request for a distribution from an account; periodic reviews and updates; a vulnerability management plan; and annual penetration tests.

Business Resiliency Program Which Effectively Addresses Business Continuity, Disaster Recovery and Incident Response

Business resiliency is the ability to quickly adapt to disruptions while maintaining continuous business operations and safeguarding people, assets and data. Plan sponsors should, at minimum, have in place a Business Continuity Plan, a Disaster Recovery Plan, and an Incident Response Plan.

I asked Aditi Group how high of a priority should business continuity, disaster recovery and incident response be to plan sponsors/plan fiduciaries? "The greatest chance for a criminal to get into your system is when you aren't looking," replied Mayeshiba. "You're too busy with an earthquake, storm, flooding, etc. A plan for everyone to lock down the data when an exogenous event occurs is critical."

"Given the potential financial and reputational impact of cyber incidents, the Business Resiliency Program should be treated as a high priority by plan sponsors and fiduciaries," informed Adriana. "Investing in proactive measures, including cyber insurance, demonstrates a commitment to protecting the organization, its stakeholders, and the beneficiaries of the plan. It also helps fulfill their fiduciary duty to act in the best interest of the plan participants and beneficiaries by safeguarding their data and assets."

Encryption of Sensitive Data Stored and in Transit

It's no secret that the best way to protect non-public information is to encrypt it. Organizations should implement current, prudent standards for encryption keys, message authentication and hashing to protect the confidentiality and integrity of the data at rest or in transit.

Strong Technical Controls Implementing Best Security Practices

Technical security solutions are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. Best practices for technical security, again, consistent with ABC/Aditi recommendations, include: Keeping your hardware, software and firmware models and versions up to date; using reputable vendor-supported firewalls, intrusion detection and prevention tools or appliances; using current and regularly updated antivirus software; implementing routine patch management (preferably automated); implementing network segregation; using system hardening; and having routine data backup (preferably automated).

Responsiveness to Cybersecurity Incidents or Breaches

It's usually not if, but when a cybersecurity breach or incident occurs, and when it does, you should be taking appropriate actions to protect the plan and it's participants, including: informing law enforcement; notifying the appropriate insurer; investigating the incident; giving affected plans and participants the information necessary to prevent or reduce injury; honoring any contractual or legal obligations with respect to the breach, including complying with notification requirements; fixing the problems that caused the breach to prevent its recurrence.

Online Security Tips

The third of the three DOL Guidances provided online security tips, which are 100% consistent with our current training tips provided by ABC and Aditi Group. The guidance states that you can reduce the risk of fraud and loss to your retirement account (or other plans), if you follow their (and our) online security tips, including registering, setting up and routinely monitoring your online account, using strong and unique passwords, using multi-factor authentication, keeping personal contact information current, closing or deleting unused accounts, being wary of free wifi, being aware and taking efforts to eliminate or reduce phishing attacks, using antivirus software and keep apps and software current, and knowing how to report identity theft and cybersecurity incidents.

Of course, phishing attacks are aimed to trick you into sharing your passwords, account numbers, and sensitive information, which allow the "bad actors" to gain access to your accounts. You should always be aware of these, and train your staff to be wary of messages that may look like it comes from a trusted organization, to lure you into clicking on a dangerous link or passing along confidential information. Warning signs include a text message or email that you didn't expect or that comes from a person or service you don't know or use; spelling errors or poor grammar; mismatched links (a link that sends you to an unexpected address; watch for those by hovering your mouse over the link *without clicking on it*, so that your browser displays the actual destination); shortened or odd links or addresses; an email request for your account number or personal information; offers or messages that seem too good to be true, express great urgency, or are aggressive and perhaps scary; strange or mismatched sender addresses; or anything else that makes you feel uneasy.

We always suggest that you check with your IT department or your Security Officer if something doesn't look or feel right, and always be cautious, and DON'T CLICK unless you are 100% sure that the email is legitimate.

I asked Aditi if there were additional tips/suggestions for online safety they'd like to share, in addition to what is stated in the guidance. "The tips are all good ones," stated Flittner. "But there are other factors to remember, such as the security of the device they are using. Is it shared with others? Is it up to date with security patches and releases? Is it still supported? Think Microsoft Windows 7, not end of life for software updates. Does it have other vulnerable software on it that hackers can exploit (think multiplayer games for example)? Be aware of who may be looking over your shoulder when you are online as well. Keep it to yourself. Don't look for anti-virus alone to catch all malware that you might innocently download or flaws that hackers may exploit. Reduce risks in ALL areas".

Overall Policies and Procedures for Cybersecurity and Their Importance

All three sets of guidance are very helpful and much-needed. I for one have been saying (and writing) for years that we needed more federal action and guidance on privacy and security. Knowing that the DOL/EBSA has made it clear that plan sponsors and fiduciaries need to pay more attention to cybersecurity, and adding this to DOL audits, should hopefully increase overall awareness and prioritize cybersecurity as plan sponsors prioritize protecting their other assets. It does make me feel good that the DOL has affirmed everything we've been teaching for so many years in our electronic security training. I asked Aditi if they feel it's about time that the government stepped up their requirements for cybersecurity.

"Absolutely," replied Flittner. "Can we get an AMEN?!"

"Plan sponsors and plan fiduciaries should indeed give serious consideration to the Department of Labor's requirement for Cybersecurity Policies and Programs," stated Adriana. "Cyber threats pose a substantial risk to ERISA plans, and it is crucial for sponsors to prioritize the protection of assets, compliance, and safeguards."

Marilyn commented: "Let's just say *the time is right* to make this a priority."

The bottom line is, had Colonial Pipeline, Anthem, a myriad of health insurance companies and providers and many others practiced what this guidance is asking plan sponsor and plan fiduciaries to do, their breaches and ransom situations may not have happened, or may have been mitigated sooner and been less costly. So, learn from those who didn't practice the policies and procedures and awareness of the importance of cybersecurity in the past, and hopefully, your data will be protected. ##

Author's Note: This article has been edited from its original version for use in CAHIP-OC's THE COIN. I'd like to thank Marilyn Monahan, Aditi Group and Adriana Mendieta for their assistance with this article. Marilyn can be reached at Marilyn@monahanlawoffice.com, Ted Flittner can be reached at ted.flittner@aditigroup.com, Ted Mayeshiba at ted.mayeshiba@aditigroup.com, and Adriana Mendieta at adriana@mendieta.net.

Editor's Note: The author can be reached at (714) 693-9754 x 3, or toll free at 866 658-3835, or by email at dmcociu@advancedbenefitconsulting.com. Advanced Benefit Consulting has tools available for purchase, including a Service Provider Questionnaire. Contact Dorothy Cociu at dmcociu@advancedbenefitconsulting.com. Be sure to listen to ABC's informative benefits and compliance podcast, the Benefits Executive Roundtable, to stay up to date. It can be found on all major podcast platforms, and ABC begins Season 5 in September, 2023.

CAHIP-OC and California State Win Big in New Orleans at NABIP Annual Convention 2023!

At the NABIP Awards Ceremony, California and CAHIP-Orange County were big winners in overall chapter awards.

California State Awards:

Landmark Award
Presidential Citation Award: Sue Wakamoto-Lee (CAHIP outgoing President and CAHIP-OC Member)
Membership Highest Retention Rate, Large State: California 82.83%
State Website Award

CAHIP-Orange County Awards:

Pacesetter Award
Presidential Citation Award: Pat Stiffler
Media Relations Award
William F Flood Public Service Award
Robert W Osler Professional Development Award

In other NABIP Convention news, the 2023 NABIP Annual Convention included great networking, educational opportunities, an LPRT cruise, the Gordon Memorial Dinner and more!

A new NABIP President, Eric Kohlsdorf, was elected. NABIP honored two Gordon Memorial Winners, Tom Harte and Dave Mordo for 2022 and 2023, which is the highest honor bestowed by the health insurance industry.

Following an extensive national search, Jessica Brooks-Woods, MPM, PHR, has been appointed as the incoming CEO of the National Association of Benefits and Insurance Professionals (NABIP), assuming her role on September 1, 2023. In her capacity as CEO, Brooks-Woods will provide strategic guidance and leadership to the staff in Washington DC and oversee the representation of licensed health insurance agents, brokers, general agents, consultants and benefits professionals through 200 state and local chapters across the country.

With a wealth of experience as a business leader, health equity advocate and benefits expert, Brooks-Woods is well-positioned to drive NABIP's mission forward. "Jessica brings nearly 20 years of experience, not only as a business leader but also as a health equity advocate and benefits expert, to NABIP," said NABIP President Eric Kohlsdorf. "The Board looks forward to working with Jessica as the association continues to shape the future of healthcare."

Brooks-Woods founded the Executive Action and Response Network (EARN) and EARN Staffing Solutions, a full-service DEI-centered consulting and talent-placement firm that played a crucial role in fostering diversity, equity and inclusion within the business community. Her previous role as president and CEO of the Pittsburgh Business Group on Health (PBGH) from 2013 to 2022 showcased her exceptional leadership. While there, she redefined and advanced healthcare value, access, equity and quality on behalf of employers. Under her stewardship, PBGH consistently achieved financial gains, delivering millions of dollars in annual savings to both employers and employees.

Brooks-Woods earned her master's degree in public management from Carnegie Mellon University and serves on various boards, including the Board of Governors for the University of Pittsburgh Institute of Entrepreneurial Excellence. Her extensive industry expertise and unwavering dedication to healthcare led to her appointment as a board member of the Pennsylvania Health Insurance Exchange.

Janet Trautwein's decision to step down and pursue new opportunities was met with gratitude from the NABIP Board of Trustees, who recognized her exceptional 26 years of service and leadership within the organization. NABIP Past President Kelly Fristoe expressed his appreciation, stating, "Janet has led NABIP through a remarkable transformation. Her deep health expertise, fierce advocacy and longtime commitment to the profession will be missed."

"The association's Trustees, staff and members are excited to welcome Jessica as the new CEO in September," said Trautwein. "I have thoroughly enjoyed working with our staff and members for the last 26 years, and I am excited to see Jessica build upon our work, leveraging her industry and DEI expertise, as she leads the premier association for health insurance and employee benefits professionals."

"I'm honored and thrilled to join NABIP as its incoming CEO. With our shared commitment to high-quality, affordable healthcare, I am excited to collaborate closely with the talented staff, dedicated members and esteemed Board of Trustees. Together, we will make a significant impact, enhancing the lives of millions across the nation," said Brooks-Woods.

The announcement was made at NABIP's Annual Convention in New Orleans on Tuesday morning, June 27, when members met Brooks-Woods and celebrated Trautwein's tenure and service to the association. ##

NABIP Conference Photos
New Orleans, LA
June, 2023

Top: Cruise Entertainment; Dave & Shauna Benson; Bob Stiffler, Dorothy Cociu, Pat Stiffler & John Evangelista. Bottom: Dorothy Cociu, John Evangelista, Pat & Bob Stiffler; Dorothy Cociu and Melissa Calibrettta

CAHIP-OC Board of Directors and Staff 2023-2024

Contact Information

EXECUTIVE BOARD

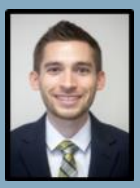
PRESIDENT
John Evangelista, LPRT
Colonial Life
Tel: (949) 452-9206
John.evangelista@coloniallifesales.com

IMMEDIATE PAST-PRESIDENT
Patricia Stiffler, LPRT
Options in Insurance
Tel: (714) 695-0674
keystonepatty@aol.com

VP of COMMUNICATIONS & PUBLIC AFFAIRS
Dorothy Cociu, RHU, REBC
Advanced Benefit Consulting
Tel: (714) 693-9754
dmcociu@advancedbenefitconsulting.com

VP of FINANCE/SECRETARY GOLF CHAIR
Juan Lopez
Colonial Life / AGA
Tel: (714) 357-0600
Juan.lopez1@me.com

VP of LEGISLATION
David Benson, LUTCF
DCB Insurance Services
Tel: (949) 328-9110
david@dcbins.com



VP of MEMBERSHIP
David Ethington
Integrity Advisors
Tel: (714) 664-0605
david@integrity-advisors.com

VP of POLITICAL ACTION
Cathy Daugherty
BAIS Insurance
Tel: (818) 865-6800
cathy@baisins.com

VP of PROF DEVELOPMENT
Ciaran O'Neill Patrick
Patrick & Patrick Insurance Services
ciaran@patricandpatrickinsurance.com

EXECUTIVE DIRECTOR
Gail James Clarke
Gail James Association Mgmt.
Tel: (714) 441-8951, ext. 3
orangecountyahu@yahoo.com

GENERAL BOARD MEMBERS

AWARD/HISTORIAN
Sarah Knapp
Colonial Life
Tel: (949) 463-8383
sarah.knapp@coloniallifesales.com

MEMBER RETENTION
Linda Madril
MIB Benefit Plans
Tel: (949) 230-4210
lgmadril@westerndental.com

SPONSORSHIP
Louis Valladares
Applied General Agency
Tel: (714) 348-0255
lvalladares@appliedga.com

SENIOR SUMMIT CHAIR
Maggie Stedt, CSA, LPRT
Stedt Insurance Services
Tel: (949) 492-8234
mstedt@stedtinsurance.com

VANGUARD
John Austin
CHOICE Administrators
Tel: (714) 542-4200
Jaustin@choiceadmin.com

SOCIAL MEDIA
Adriana Mendieta
Cyber Insurance Solutions
Tel: (562) 404-0672
adriana@mendieta.net

Why Get Involved in CAHIP-OC?

- *Learn more about our industry*
- *Become a better consultant to help your clients*
- *Network with professionals in all areas*
- *Be a resource to your colleagues*
- *Make an impact with legislation*

HIPAA Updates, Continued from Page 8

iHealth Solutions has paid $75,000 to OCR and agreed to implement a corrective action plan, which identifies steps iHealth Solutions will take to resolve potential violations of the HIPAA Privacy and Security Rules and protect the security of electronic protected health information. Under the terms of the settlement agreement, iHealth Solutions will be monitored by OCR for two years to ensure compliance with the HIPAA Security Rule. iHealth Solutions has agreed to take the following steps:

- Conduct an accurate and thorough analysis of its organization to determine the possible risks and vulnerabilities to the electronic protected health information it holds;

- Develop and implement a risk management plan to address and mitigate identified security risks and vulnerabilities to the confidentiality, integrity, and availability of its electronic protected health information;

- Implement a process to evaluate environmental and operational changes that affect the security of electronic protected health information; and

Develop, maintain, and revise, as necessary, its written HIPAA policies and procedures.

The resolution agreement and corrective action plan may be found at: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/ihealth-ra-cap/index.html.

On June 15, 2023, the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) announced a settlement with Yakima Valley Memorial Hospital, a not-for-profit community hospital located in Yakima, Washington resolving an investigation under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). OCR investigated allegations that several security guards from Yakima Valley Memorial Hospital impermissibly accessed the medical records of 419 individuals. HIPAA is a federal law that protects the privacy and security of protected health information. The HIPAA Privacy, Security, and Breach Notification Rules apply to most health care organizations and set the requirements that HIPAA-regulated entities must follow to protect the privacy and security of health information. To voluntarily resolve this matter, Yakima Valley Memorial Hospital agreed to pay $240,000 and implement a plan to update its policies and procedures to safeguard protected health information and train its workforce members to prevent this type of snooping behavior in the future.

"Data breaches caused by current and former workforce members impermissibly accessing patient records are a recurring issue across the healthcare industry. Health care organizations must ensure that workforce members can only access the patient information needed to do their jobs," said OCR Director Melanie Fontes Rainer. "HIPAA

Continued on page 31

MEMBERSHIP NEWS

We'd like to welcome the newest members of CAHIP-OC!

Susan Baker	**Ciaran O'Neill-Patrick**	**Richard Cano**
David Hunter	**Anne Kelly**	**Glenda Collins**
Ryan Clear	**Tim Johnson**	
Brittany Perreira	**Lilian Marin**	

Interested in Joining? Many ways to join:

- **Contact our Membership Team:**

David Ethington
Integrity Advisors
Tel: (714) 664-0605
david@integrity-advisors.com

Agency Memberships Now Available!

- **Talk to a Board Member**

(see page 22 for board roster)

JOIN CAHIP-OC

Come Explore the Medicare Jungle at the Senior Summit! August 22-24, 2023

By: Maggie Stedt, C.S.A. LPRT, Medicare Summit Chair

Come join us at the Pechanga Resort and Casino August 22nd to August 24th for the 11th Annual Senior Summit! Located in Temecula, off of the 15. It is easy to travel to from the Inland Empire, San Diego, Orange County, Los Angeles and the Ontario and San Diego airports. This year we are excited to announce that we will have two outstanding keynote speakers! Bill Cates will help you explore ways to grow the number of referrals you receive and to increase your business with personal introductions. Tony Rubleski will present "How to Positively Disrupt Your Mind-Set and Business." You will learn how use social media platforms more effectively and to create a business identity that will distinguish you from your competition! It is time to focus on growing your business, while learning about new programs and product offerings by our carriers.

We start off on Monday, August 21st for those who want to golf at the outstanding, challenging golf course at Pechanga. A separate reservation is needed to participate in this fun event. Simply go to www.theseniorsummit.net for more information. On Tuesday, we start right off with a panel presentation and CE and other classes to up your game in the Medicare Jungle! Brad Miles is returning this year with a deep dive into the tools available to you on the www.medicare.gov website. Stan Isreal will provide information about CA initiatives regarding Long Term Care. Our Exhibit Hall opens up on Tuesday afternoon and continues through the Summit! Wednesday we will take a deep dive into the Federal and State regulations and challenges, especially the CMS Marketing Regulations for this year's upcoming Annual Open Enrollment! Faith Borges, John Greene, Nick Uehlechke and Tim Kantor are gearing up to provide you with the timely updates. Thursday will continue with more classes and information you need, such as the changes in the Medicare/MediCal offerings and opportunities!

Breakfast will be served Tuesday, Wednesday and Thursday and lunch is included on Tuesday and Wednesday. Dinners are on your own to explore the Casino's restaurants or perhaps a quick trip to a local winery or the restaurants in nearby Temecula. Pechanga continues to offer our attendees special room rates, but you need to reserve early to make sure you are in!

As our program is being fleshed out at the time of writing this article, go www.theseniorsummit.net website for up-to-date information and to sign up to attend this great event. We also have opportunities for sponsors and exhibitors. A big Thank-You to our Gold Ribbon Sponsor, Applied General Agency; our Red Ribbon sponsors Alignment Health, Golden Outlook and Humana; our White Ribbon Sponsor Wellcare; our Blue Ribbon Sponsors Brand New Day/Central Health Plan and Aetna Medicare; and, to all of our sponsors and exhibitors, who make it possible to offer your this event. *Come Join Us!* ##

KEYNOTE SPEAKERS AT MEDICARE SUMMIT:

*Tony Rubleski is currently the president of **Mind Capture Group.** His message is designed to help people 'Capture' more minds and profits. He is a bestselling author, and creator of the **Mind Capture Bootcamp** now in its 12th year. He has over 25+ years of experience in the personal development industry.*

His Mind Capture book series has spawned multiple bestsellers in a variety of business and coaching categories with Amazon.com.

Join us at The Senior Summit to hear Tony discuss how to become more profitable on August 22, 2023.

Bill Cates, CSP, CPAE, works with financial professional to speed up their growth without increasing their marketing budget. Professionals tap into Bill's proven process to multiply their best clients through introductions from clients and Centers of Influence and communicate their value proposition more effectively. Bill helps professionals move from push prospecting to magnetic marketing – to attract more ideal clients.

Join us for Bill's Keynote Address on August 23, 2023.

Don't Miss This Informative Summit!

August 22 to 24, 2023
at Pechanga Resort Casino, Temecula, CA

Register today for this important Medicare Summit! A full 3 days of educational certifications and classes, informative panel discussions with guest speakers who are sure to give you all the tools you will need to be a successful Medicare agent. Plus breakout sessions and exhibitors including various insurance carriers, medical groups, and supplemental benefit providers all ready to share their information. It's a great way to network, meet in person and talk to the different representatives.

Scan this Code to Register Today!

Breakout Sessions, Training Programs, and discussions about the new Medicare Legislation both state and federal for 2024

Visit our website: theseniorsummit.net

NABIP | pac

NABIP PAC has a new name but it remains committed to moving forward and fulfilling its mission to support candidates that support our industry. I'm writing today to explain what NABIP's political action committee is and how it operates.

What is the National Association of Benefits and Insurance Professionals Political Action Committee (NABIP PAC)?

- NABIP PAC is a separate segregated fund (SSF) that allows for political advocacy from the connected organization -- in this case, NABIP.
- For this reason, the PAC (candidate fund) is restricted to raising money from dues-paying members.
- PAC money is NOT tax-deductible. Contributions are not deductible for state or federal tax purposes.
- NABIP PAC has two different accounts:
  - Candidate Account
  - Administrative Fund

What is the Candidate Account?

- It is made up of individuals' contributions through personal credit cards or bank accounts.
- Funds from this account are given to political candidates, both challengers and incumbents, Democrats and Republicans.
- NABIP members, their spouses and NABIP staff can give up to $5,000 each year (federal law).

What is the Administrative Fund?

- Businesses can contribute to the Admin Fund.
- State and local chapters can also contribute.
- Money in this account goes to the operating costs of NABIP PAC so that the Candidate Account can be reserved solely for political contributions.
- Unlike the Candidate Account, there are no contribution limits on the Administrative Fund.

How does the NABIP PAC money we donate get spent by candidates?

- Winning Senate candidates spent an average of $16 million in 2022.
- On average, $2.0 million was spent to win a House seat in 2022.
- A NABIP PAC donation of $2000 is just one in 2000 groups of people contributing to total amount needed to win that House seat.
- Needless to say, members of Congress have many groups like NABIP that expect their legislative agendas to become a priority through their donation.
- **Through NABIP PAC, NABIP gets time and access to members of Congress to advocate on behalf of agents and brokers.**

What are the rules for communication of available money for Candidate Account Fund?

- A member of Congress and his or her staff are never allowed to discuss the campaign or fundraising while using government resources. This includes in their office, while they are working on a Congressional activity, or using an email or phone number provided by the member's office.

Reach out to me Cathy@BAISins.com or Gail to view/ or update your NABIP-pac fund giving level here and donate today if you are not currently!

Cathy Daugherty , VP of PAC

Are you Ready to Contribute NABIP PAC?

If so, please complete the form on page 27!

Note: CAHIP PAC contribution form can be found on page 33!

NABIP | pac

The purpose of the NABIP PAC is to raise funds from NABIP members to support the political campaigns of candidates who believe in private-sector solutions for the health and financial security of all Americans.

Contribute securely at www.nabippac.org

Step 1: Tell us about yourself. *(All information must be completed in full by contributor.)*

Name: Occupation:

Employer: Address:

Email: Phone:

Step 2: Please select (A) Fund (B) Frequency (C) Contribution Level

☐ New Contributor ☐ Past Contributor ☐ Change Contribution to Amount Checked Below

A. Choose a Fund

☐ Candidate Fund* ☐ Administrative Fund**

**Candidate Fund can ONLY accept personal contributions.*
***Administrative Fund can accept corporate contributions.*

B. Contribution Frequency

☐ One-Time Contribution
☐ *Charge my account annually for this amount.*

☐ Monthly Contribution (Recurring)
Credit card or bank account will be charged monthly.

C. Contribution Levels

		(Annual)		*(Monthly)*
Member	☐	$150	☐	$12
Bronze	☐	$365	☐	$30
Silver	☐	$500	☐	$42
Gold	☐	$750	☐	$63
Platinum	☐	$1,000	☐	$85
Diamond	☐	$2,000	☐	$170
Double Diamond	☐	$3,000	☐	$250
Triple Diamond	☐	$5,000	☐	$415
Amount not listed	☐	$	☐	$

Did a NABIP member refer you? If so, who?

Step 3: Provide your method of payment.
(Payment must be from a personal credit card or bank account if contributing to the Candidate Fund.)

Credit or Debit Card ☐ American Express ☐ Discover ☐ Mastercard ☐ Visa

Card Number: Expiration Date: (mm/yy):

CVV: Zip Code:

Checking Account

Bank Routing Number: Account Number:

Signature

☐ I authorize NABIP PAC to initiate charges to my personal bank account or credit card as shown above.

Signature: Date:

Step 4: Submit this form.

Mail
NABIP PAC
999 E Street NW, Suite 400
Washington, DC 20004

Fax
202-747-6820

Email
nabippac@nabip.org

A contribution to a Political Action Committee is not tax deductible. Only NABIP members, their immediate families and NABIP staff may contribute. Only U.S. citizens and permanent residents may contribute. Any guidelines mentioned for contributions are merely suggestions. You may contribute more or less than the guidelines suggest, and the National Association of Benefits and Insurance Professionals (NABIP) will not favor nor disadvantage you by reason of the amount of your contribution or your decision not to contribute. Federal law requires PACs to report the name, mailing address, occupation and employer for individuals whose donations exceed $200 in a calendar year. Federal law prohibits corporate or business donations to a federal PAC. Please make certain that your check or credit card is your personal account.

NABIP Annual Convention 2023 Photos

National Association of Benefits and Insurance Professionals

NABIP

Shaping the *future* of healthcare

How to get more value from your NABIP membership

The activities below provide a blueprint for extracting the greatest value from your membership:

- Visit NABIP's Micro Site - **www.welcometonabip.org**
- Take advantage of NABIP's **Mentorship Program**
- Read America's Benefit Specialist Magazine each month and learn something new
- Listen to the NABIP **Healthcare Happy Hour Podcasts** on a weekly basis for up-to-date talking points
- Attend the NABIP **Power Hour** webinar monthly for in depth topic discussions and socialize with fellow members
- Attend Local Chapter meetings for opportunities to learn and network
- Volunteer to serve on a committee (Membership, Social, Programs/Expo, Legislative, etc.)
- Recruit one new member – best way to learn is to teach someone else about the NABIP value proposition
- Meet with a NABIP Board member and find out what motivates them to give their time and money
- Attend Day on the Hill and meet with your state legislators to discuss bills you support or oppose
- Attend NABIP Capitol Conference – annual legislative fly-in to Washington DC (IMPORTANT ONE)
- Attend NABIP Annual Convention to meet members from across the country and vote for NABIP incoming Secretary and other membership matters
- Contribute to NABIP-PAC – Political Action Committee contributions help us to have our voice heard on legislative issues at the national and state level. Contribute monthly to each!
- Participate in Operation Shout – click and sign letters to **your** elected officials regarding important grass roots efforts
- Earn your **Registered Employee Benefits Consultant** designation - acquired from The American College
- Complete all 12 modules of the **Leadership Academy**.
- Sign up to receive **Broker 2 Broker** emails on NABIP.org where you can post questions and respond to fellow members from around the country
- Share with your clients that you are a member of NABIP and working to protect their access to private health insurance and other benefits!

More information at www.nabip.org

NABIP Operation Shout! One of the primary ways we engage in advocacy for the consumer is by supporting legislation that ensures the future and stability of the insurance industry. Through Operation Shout, you as a member have the opportunity to participate in this process. As legislative needs arise, you will be prompted by staff to participate in Operation Shout. Participating is quick and easy. When you click on "write" you will have the option of using the message we have already created, which takes less than a minute, or composing your own. Either method is effective and sends a strong message to your member of Congress about the important issues facing us today. You can also check back at any time to view and send archived messages. When engaging in NABIP grassroots operations, remember that we are most effective when we speak with one voice. As always, if you have any questions, please feel free to contact us!

covered entities must have robust policies and procedures in place to ensure patient health information is protected from identify theft and fraud."

In May 2018, OCR initiated an investigation of Yakima Valley Memorial Hospital following the receipt of a breach notification report, stating that 23 security guards working in the hospital's emergency department used their login credentials to access patient medical records maintained in Yakima Valley Memorial Hospital's electronic medical record system without a job-related purpose. The information accessed included names, dates of birth, medical record numbers, addresses, certain notes related to treatment, and insurance information.

As a result of the settlement agreement, Yakima Valley Memorial Hospital will be monitored for two years by OCR to ensure compliance with the HIPAA Security Rule. Yakima Valley Memorial Hospital has agreed to take the following steps to bring their organization into compliance with the HIPAA Rules:

- Conduct an accurate and thorough risk analysis to determine risks and vulnerabilities to electronic protected health information;
- Develop and implement a risk management plan to address and mitigate identified security risks and vulnerabilities identified in the risk analysis;
- Develop, maintain, and revise, as necessary, its written HIPAA policies and procedures;
- Enhance its existing HIPAA and Security Training Program to provide workforce training on the updated HIPAA policies and procedures;

Review all relationships with vendors and third-party service providers to identify business associates and obtain business associate agreements with business associates if not already in place.

The resolution agreement and corrective action plan may be found at: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/yakima-ra-cap/index.html.

On June 5, 2023, the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR) announces a settlement with Manasa Health Center, LLC, a health care provider in New Jersey that provides adult and child psychiatric services. The settlement resolves a complaint received by OCR in April 2020, alleging that Manasa Health Center impermissibly disclosed the protected health information of a patient when the entity posted a response to the patient's negative online review. Following an OCR investigation, potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule include impermissible disclosures of patient protected health information in response to negative online reviews, and failure to implement policies and procedures with respect to protected health information. Manasa Health Center paid $30,000 to OCR and agreed to implement a corrective action plan to resolve these potential violations.

"OCR continues to receive complaints about health care providers disclosing their patients' protected health information on social media or on the internet in response to negative reviews. Simply put, this is not allowed," said OCR Director Melanie Fontes Rainer. "The HIPAA Privacy Rule expressly protects patients from this type of activity, which is a clear violation of both patient trust and the law. OCR will investigate and take action when we learn of such impermissible disclosures, no matter how large or small the organization."

OCR opened an investigation in response to a complaint by a patient alleging that Manasa Health Center posted a response to the patient's negative online review that included specific information regarding the individual's diagnosis and treatment of their mental health condition. In addition to the patient who filed the complaint, OCR's investigation found that Manasa Health Center impermissibly disclosed the protected health information of three other patients in response to their negative online reviews. OCR's investigation also found that Manasa Health Center failed to implement HIPAA Privacy policies and procedures.

In addition to the monetary settlement, Manasa Health Center will undertake a corrective action plan that will be monitored for two years by OCR to ensure compliance with the HIPAA Privacy Rule. The corrective action plan includes the following steps:

- Develop, maintain, and revise its written policies and procedures to comply with the HIPAA Privacy Rule,
- Train all members of Manasa Health Center's workforce, including owners and managers, on the organization's policies and procedures to comply with the HIPAA Privacy and Security Rules,
- Within 30 calendar days of the agreement, Manasa Health Center shall issue breach notices to all individuals, or their personal representatives, whose protected health information is disclosed on any internet platform without a valid authorization, and

Within 30 calendar days of the agreement, Manasa Health Center shall submit a breach report to HHS concerning individuals whose protected health information is disclosed on any internet platform without a valid authorization.

The resolution agreement and corrective action plan may be found at: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/.manasa-ra-cap/index.html. ##

WHAT IS THE ANNUAL VALUE OF NAHU MEMBERSHIP?

NAHU is now NABIP!

Support CAHU PAC!

You don't have to be a member to contribute to the PAC!

CAHU-PAC advocates on behalf of licensed insurance agents and their clients in California on numerous issues of vital concern including their role in solicitation of health, long-term care, annuity and life insurance products, insurance market reform, rising health care costs and regulations affecting agents and brokers.

NABIP Healthcare Happy Hour

Subscribe to NAHU's Healthcare Happy Hour

http://nahu.org/membership-resources/podcasts/healthcare-happy-hour

Latest Podcasts:

- **House Ways & Means Committee Advances NABIP Federal Priority to Ease Employer Reporting Process**
- **Are you Ready for NABIP's Annual Convention?**
- **How to Best Leverage Employee Benefit Portfolios—from Retirement Plans to Pet Insurance**
- **A Stay inn ACA Preventive Care Mandate Case: NABIP Submits More Testimony**
- **What You Need to Know About the End of the COVID-19 Emergency Periods**
- **NABIP Submits Written Testimony on Host of Healthcare Issues**
- **Special Guest from Nonstop Health Discuss Benefits for Brokers and Employers**
- **An Individual Market Agent's Perspective on the Medicaid Unwinding**

Two Must-Attend Events!

Mark Your Calendars Now!

August 22-24, 2023

Senior Summit

Pechanga Resort Casino, Temecula

September 12, 2023

CAHIP-OC CE Day

Lake Forest Community Center

Earn 5 CE Credits—2 Tracks!

1) Group & Compliance

2) Medicare, Individual, Life & Annuities

California Association of Health Underwriters Political Action Committee
2520 Venture Oaks Way, Ste 150
Sacramento, CA 95833
FPPC # 892177

CAHU PAC CONTRIBUTOR COMMITMENT FORM

LAST NAME FIRST NAME MIDDLE

OCCUPATION (Required for FPPC reporting purposes)

EMPLOYER (if self employed, name of business; Required for FPPC reporting purposes)

WORK ADDRESS (Please provide street address only, no P.O. Boxes) ☐ Check if address for Credit Card

CITY, STATE, ZIP PHONE FAX

HOME ADDRESS (Please provide street address only, no P.O. Boxes) ☐ Check if address for Credit Card

CITY, STATE, ZIP PHONE FAX

CONTACT EMAIL ADDRESS LOCAL CHAPTER

PRECIOUS GEM STONE CONTRIBUTION LEVELS

Levels	Annual	Monthly Minimum	Diamond Levels	Annual	Monthly Minimum
Ruby	$250 - $499	$21/month	One Star	$1,000 - $1,999	$85/month
Emerald	$500 - $719	$42/month	Two Star	$2,000 - $2,999	$170/month
Sapphire	$720 - $999	$60/month	Three Star	$3,000 - $3,999	$250/month
			Four Star	$4,000 - $4,999	$340/month
			Five Star	$5,000 - $6,000	$420/month

NOTE: POLITICAL CONTRIBUTIONS ARE REPORTED TO THE FPPC. YOUR NAME, AS A CONTRIBUTOR, WILL BE A MATTER OF PUBLIC RECORD.

PAYMENT METHOD: (attach check or select method below)

Payment Method	Card or Account #	Exp. Date	Security Code	Monthly Amount	One-Time Contribution
Check Enclosed					$
Visa/MC/Amex				$	$
Auto-checking withdrawal	PLEASE ATTACH A VOIDED CHECK			$	

Bank Draft / Credit Card Authorization: *I (we) hereby authorize the CAHU PAC to initiate debt entries to my (our) checking account and or credit card. Monthly or one-time debits to be made as shown above. Monthly contributions will continue to be drawn until CAHU PAC is notified in writing to cease. I understand that if I should request changes to the amount withdrawn or a cancellation of these charges that it may be 30 days before these changes to become effective.*

Signed: _____ ***Date:*** _____

Please return this PAC Commitment Form to:
Mail: CAHU PAC 2520 Venture Oaks Way, Ste 150, Sacramento CA 95833
FAX: (916) 924-7323 Questions: (800) 322-5934

Revised: 10/2019

SPECIAL THANKS TO OUR ANNUAL CORPORATE SPONSORS!

Titanium Level

KAISER PERMANENTE®

aga
AN INTEGRITY COMPANY

Gold Level

Anthem®
Independent licensee of the Blue Cross Association.

Clarity | BENEFIT SOLUTIONS™

Silver Level

COVERED CALIFORNIA
SMALL BUSINESS

Providence
Medicare Advantage Plans

Bronze Level

BRi

Word&Brown®

Medicare Agents!

In today's world, you must have access to and be properly trained on using remote enrollment tools.

AGA's Agent Portal gives you access to your own suite of online tools available anywhere you have the internet. It's a one-stop shop for all your Medicare business needs.

- Your Personal Plan Finder platform
- Quote ALL plans
- Enroll remotely
- Text SOAs

Call today!

1-844-SALES-UP

www.appliedga.com

aga

1442 E. Lincoln Ave., PMB 441
Orange, CA 92865-1934

- THE C.O.I.N. -

Don't miss our upcoming events!

UPCOMING EVENTS

Region VIII Leadership Conference
- Hilton Anaheim, CA

AUGUST 6-7 2023

11th Annual Senior Summit
- Pechanga Resort Casino

AUGUST 22-24 2023

CAHIP-OC CE Day
- Lake Forest Community Center

SEPTEMBER 12, 2023

Visit our website for more details

www.ocahu.org

linkedin.com/groups/4100050 **facebook.com/OCAHU** **@OrangeCountyAHU**