

PLUS: DEI AND DATA/LIFE SETTLEMENTS/VIRTUAL ASSISTANTS

CALIFORNIA BROKER

VOLUME 40, NUMBER 9

Serving California's Life/Health Profession

JUNE 2022

A large, stylized bomb is the central focus. The bomb's body is covered in a green digital code pattern of binary digits (0s and 1s). The top of the bomb is a dark, cylindrical cap with a handle. From the handle, a plume of digital smoke or fire, rendered in shades of orange, yellow, and red, billows out. The bomb is set against a white background with a subtle grid pattern.

CYBERSECURITY 2.0

**The Latest on
Cyber-Attacks,
Ransomware and the
Need for
Risk Assessments - p. 14**



Together we offer even more!

brand new day

A Bright HealthCare Company



CENTRAL HEALTH
MEDICARE PLAN

27 Plans in 24 Service Areas Across California!

- Embrace CSNP - for Medicare beneficiaries with a chronic condition of cardiovascular disease or diabetes
- Savings Plan - for Medicare beneficiaries that want good coverage and a \$125 monthly Part B rebate
- Valor Plan - for Medicare beneficiaries that have Rx coverage elsewhere and want a \$140 Part B rebate
- Medi-Medi Plan - for Medicare beneficiaries with Medicare and Medi-Cal
- Many other plans for your Medicare clients

Ready to learn more?

Contact Broker support today!

Brand New Day

1-866-255-4795 Ext. 2018

bndhmo.com/brokers

Central Health Plan

1-626-388-2375

centralhealthplan.com/broker



David Milligan
VP of CA Sales

THAT CALIFORNIA DIFFERENT FEELING.



A California Different way to think about ancillary benefits.



Quote Different | 866.412.9254 choicebuilder.com



Contents

CALIFORNIA BROKER

June 2022

12

LEGISLATION

CAHIP 2022 Capitol Summit: A chance to meet with lawmakers

With California's population heft, we super drive many of the nation's cultural trends – zoom zoom! – including how healthcare is delivered.

BY LINDA HUBBARD LALANDE

24

FRAUD

Genetic Testing Scams on the Rise — Protect Your Medicare

Last year alone, one in every four cases reported to our California Senior Medicare Patrol (SMP) was a genetic testing scam.

BY KAREN JOY FLETCHER

28

FINANCE

Leveraging Virtual Assistants for Greater Employee Satisfaction

Amid all the paperwork and reporting, advisors can feel like they have very little time to focus on the most important part of their job: client service.

BY AARON KANE

14

CYBERSECURITY

Cybersecurity 2.0 — The Latest on Cyber-Attacks, Ransomware and the Need for Risk Assessments

It's been about a year since we were all on pins and needles about cyber-attacks that resulted in gas shortages and price hikes in the East and meat and food shortages everywhere.

BY DOROTHY COCIU

26

COVID-19 TESTS

Insurers Required to Offer COVID-19 Tests At No Cost To Plan Members

Members of private insurance plans are allowed eight over the counter tests per calendar month

BY MICHAEL GIUSTI

30

COST CONTROL

Employer Healthcare Costs Lowered by Increased Transparency and Employee Engagement

In an extensive analysis of patient claims data, health plan member engagement has emerged as employers' single best-practice solution for controlling costs and improving outcomes for their employees.

BY PATTY STARR AND CRAIG KURTZWEIL



Join the Team of one of the fastest growing Medicare Advantage companies in the country!

Alignment Health Plan includes the industry first ACCESS On-Demand “Black Card” giving members’ access to 24/7 care and service OTC, grocery benefits, Healthy Rewards and so much more!



LEARN ABOUT THE PLANS THAT OFFER MORE HEALTHCARE COVERAGE OPTIONS TO MEDICARE BENEFICIARIES IN CALIFORNIA.

Working with Alignment, you will receive:



Top commissions with lifetime renewals



Local, field-based broker support with advanced Medicare expertise



Broker support, Concierge and Medicare dedicated member services!



Support staff is California-based, and 100% Alignment employees



A secure broker portal with complete transparency, including online enrollment, application status, commissions and membership reporting



Innovative product offerings. (In many areas, multi-plan offerings)

Join us and learn how adding Alignment Health Plan to your portfolio will be instrumental in growing your Medicare business this AEP and beyond.

CONTACT US TODAY!
partnerexperience@ahcusa.com
(888) 793-5700

PUBLISHER

Ric Madden
publisher@calbrokermag.com

EDITORS

Linda Lalande Hubbard
Linda.calbrokermag@gmail.com

Thora Madden
Associate Editor
Surveys
Thora@calbrokermag.com

2022 INDUSTRY CONTRIBUTING EDITORS:

Naama O. Pozniak, Louis Brownstone,
Phil Calhoun, Dorothy Cociu,
Lisa Rehbarg and Maggie Stedt

ART DIRECTOR

Randy Dunbar
Randy@calbrokermag.com

VP MARKETING

Devon Hunter
Devon@nustepinsurance.com

ADVERTISING ACCT EXEC

Cindie Klima
cindiek@gmail.com

CIRCULATION

calbrokermag@calbrokermag.com

LEGAL EDITOR

Paul Glad

EDITORIAL AND PRODUCTION:

McGee Publishers, Inc.
3727 W. Magnolia Blvd., #828
Burbank, CA 91505
(818) 848-2957

calbrokermag@calbrokermag.com

Subscriptions and advertising rates, U.S. one year: \$42. Send change of address notification at least 20 days prior to effective date; include old/new address to: McGee Publishers, 3727 W. Magnolia Blvd., #828, Burbank, CA 91505. To subscribe online: calbrokermag.com or call (800) 675-7563.

California Broker (ISSN #0883-6159) is published monthly. Periodicals Postage Rates Paid at Burbank, CA and additional entry offices (USPS #744-450). POSTMASTER: Send address changes to California Broker, 3727 W. Magnolia Blvd., #828, Burbank, CA 91505.

©2022 by McGee Publishers, Inc. All rights reserved. No part of this publication should be reproduced without consent of the publisher.

No responsibility will be assumed for unsolicited editorial contributions. Manuscripts or other material to be returned should be accompanied by a self-addressed stamped envelope adequate to return the material. The publishers of this magazine do not assume responsibility for statements made by their advertisers or contributors.

Printed and mailed by Southwest Offset Printing, Gardena, Calif.

32

COMPENSATION

Broker Friendly Carriers Are Valuable Partners

Independent brokers and agents offer their clients more solutions and gain a level of confidence with carrier partners who are proactive with member service, offer competitive plan designs, and commit to a competitively priced and robust provider network.

BY PHIL CALHOUN

34

FINANCIAL PLANNING

How Working Less Might Be Better for Your Financial and Mental Health

A money script is a belief that typically developed in childhood and is hard-wired into adult financial behaviors. There are four categories of money scripts: money avoidance, money status, money vigilance, and money worship.

BY CHIA-LI CHIEN

36

DEI AND DATA

Are you meeting the needs of your diverse populations when it comes to health benefit strategy?

A best practice in any employee health and benefit strategy, particularly those targeted at reducing ever increasing healthcare costs, is to collect Health Risk Assessment (HRA) information and use these data to drive your wellness or wellbeing programming strategy.

BY DR. TYLER AMELL

IN EVERY ISSUE

Industry News	8
Classified Advertising	46
Ad Index	46

38

DEI

Taking PRIDE: How benefits support inclusivity

June's Pride Month is a great time to celebrate our diversity and the accomplishments of the LGBTQ+ community and its advocates – but also to take stock in how well we're doing in creating a more equitable workplace.

BY ANN COSIMANO

40

AGENT'S VOICE

Positioning My Agency for Sale

Second of four installments

In this installment, I'll share the steps I took to position my agency for sale, personally and professionally.

BY AMY EVANS

42

LONG-TERM CARE

Can State Long-Term Care Plans alone solve the Long-Term Care Problem?

The impact on state Medicaid programs due to the aging population, and lack of knowledge of LTC planning, is driving folks to purchase LTC insurance.

BY CHRISTINE MCCULLUGH

44

LIFE SETTLEMENTS

How You and Your Client Benefit from Both Sides of the Life Insurance Settlement Coin

Did you know there are actually two ways that you can help your clients and potential clients with life insurance settlements?

BY LISA REHBURG WITH BRIAN J. CLARK



COVERED CALIFORNIA
SMALL BUSINESS

a partnership that pays

**BONUS PROGRAM - COVERAGE EFFECTIVE:
JULY 1, 2022 TO JANUARY 1, 2023**

Earn even more for offering your clients California's most comprehensive access to doctors and hospitals:

- 
Full Network PPOs*
 - Blue Shield
 - Health Net
- 
HMO offerings from*
 - Blue Shield
 - Kaiser Permanente
 - Sharp Health Plan
- 
NEW! CCSB offers 4-tier selection
- 
Single bill
- 
Covers enrollments across all CCSB Carriers

EARN EXTRA WHEN YOU SELL NEW SMALL GROUPS

Group Size (Enrolled Employees)	Incentive Earned
51 - 100	\$ 8,000
26 - 50	\$ 4,000
16 - 25	\$ 2,000
6 - 15	\$ 1,000

Contact your local Covered California for Small Business sales representative to learn why we're growing and how we can help build your business! An increasing number of agents and their clients are glad they did.

CoveredCA.com/ForSmallBusiness
844.332.8384

Some Key Rules:

1. Applies to new to Covered California for Small Business (CCSB) groups with initial effective dates of 07/1/22, 08/1/22, 09/1/22, 10/1/22, 11/1/22, 12/1/22 and 1/1/23
2. Bonuses will be calculated on number of subscribers (employees) in effect for the first effective month of the policy as determined by CCSB.
3. No pro-ration of target values will take place.
4. Business written through partnering General Agencies qualifies.
5. Covered California intends to issue incentive payments forty-five (45) days following the ninety (90) day requirement outlined in Section D(1)(b) of Exhibit F. Covered California may modify its payment schedule at any time.

For a complete list of the program rules go to:

<http://www.coveredca.com/agents/become-an-agent-for-small-business/CCSB-agents/>



**Insurance companies vary by region and are subject to change.*

How are you feeling? Hartford Study Shows Depressed Employees Affect Not Only Themselves, but Company Profits

The Hartford's study reveals 71% of employers feel the deteriorating mental health of their workforce is having a negative financial impact on the company.

Compounding the situation, as employers' productivity-related concerns grew, the number of employee assistance programs, wellness benefits and addiction treatment programs being offered by employers fell between 2020 to 2022.

"Our data shows an undeniable, direct correlation between employee mental well-being, mental health support, and the impact to a company's bottom line," said The Hartford's Chairman and CEO Christopher Swift. "Employers who want a contemporary, inclusive workplace that supports its people should proactively invest in mental health, with an eye to empathy and equity. The need is real, and the time is now."

Femtech Industry Connects Women to Tailored Products and Care

Demand for female-based health care is harnessing science and technology

Connecting women to resources and each other, as well as providing science-backed insights and analytics, the femtech industry is providing women with the help needed to supplement traditional care.

According to Worth.com, "Femtech — a term coined by Ida Tin, cofounder and CEO of the period-tracking app Clue — refers to the movement to create products, services and software designed to support women's health. Things like women's cycles, libido, menopause and reproductive journey are all natural aspects of women's health that are traditionally viewed as taboo topics. This can lead to a sense of isolation among many women who may not know whether something they are experiencing is normal or not. That is where femtech comes in."

Read more: worth.com/femtech-products-supporting-womens-health.

Curiosity leads to innovation

Find surprising solutions by encouraging exploration

Organizations that foster curiosity are fueling better results, growth and success.

According to innovation consultant Diana Kander (dianakander.com) in an article on ChiefExecutive.net, "Encouraging deliberate curiosity means identifying and remedying your unwitting gaps in perception, getting rid of initiatives that are not creating value, and fostering accountability among team members."

For businesses, asking these three essential questions starts the adventure:

- 1. What are your blind spots?**
- 2. How will you know what's not working?**
- 3. How do you create accountability?**

Read more: chiefexecutive.net/3-questions-ceos-should-ask-to-practice-deliberate-curiosity/



ORANGE COUNTY EXIT PLANNING INSTITUTE ADDS CALHOUN AS BOARD MEMBER

In May, Phil Calhoun of Integrity Advisors was nominated as a member of the board of directors for the Orange County Exit Planning Institute. Calhoun will be working to build connections between health benefits brokers and the Exit Planning Institute. In this effort, benefit brokers will be able to meet collaborative advisors and bring the institute's deep resources to their business owner clients. Over 70% of businesses owned by baby boomers will be sold or closed within 15 years. Passing the business on to loved ones, employees, or an outside buyer takes planning to get the best result and highest value. Calhoun is an active voice for health brokers looking to protect, grow and sell their health commissions and his book on this topic has helped many brokers plan for their future.

"Benefit brokers can be a central point of introduction with their clients to assist with this critical planning process," says Calhoun. "We're here to help." The Exit Planning Institute has chapters throughout all of California.

Contact: phil@integrity-advisors.com

Always Needing More Protection Always Needing More DI



ATTORNEYS



PHYSICIANS



GSI High Limit DI

If you are not selling GSI High Limit DI you have no idea what you're missing. Instead of the \$3,000 to \$5,000 commission cases of the individual market, the GSI market boasts regular commissions of \$300,000 to \$500,000! We are serious and there is a fortune to be made in the guaranteed-issue disability (GSI) marketplace.



PETERSEN INTERNATIONAL UNDERWRITERS
(800) 345-8816 ♦ www.piu.org ♦ piu@piu.org

It's about time the emphasis was on **Simpler and AFFORDABLE** in the New ACA Rules

CMS released the final notice of benefit and payment standards for Affordable Care Act plans for the 2023 plan year. (<https://www.beckerspayer.com/payer/new-cms-rule-aims-to-make-aca-coverage-more-accessible-affordable.html>) The rule helps simplify the consumer shopping experience by establishing standardized plan options for issuers offering qualified health plans.

All health insurance providers using state or federal ACA exchanges are **REQUIRED** to offer standardized plan options at every metal level, network type and service area starting next year to make it easier for consumers to compare plans.



We are *Real* California Brokers helping active health Brokers Protect, Grow and Sell health commissions

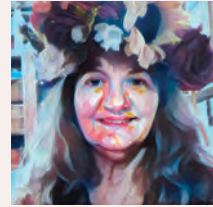
NOT SURE WHERE TO START YOUR PLANNING?
Visit our website for more details.
Learn from our clients and see how we can assist you. Then set up a free 15-minute session.
www.commission.solutions
(800)500-9799



Commission Solutions

Helping health insurance brokers **Protect, Grow & Sell** their commissions

www.commission.solutions



Changing of the Guard at California Broker

Hello, it's me – Linda Hubbard Lalande! I'm assuming the role of EDITOR in Victoria Alexander's stead for Insider News Wednesday e-blast, and our monthly print magazine.

Reach me at **Linda**, calbrokermag@gmail.com or 1-818-730-2943.

Send in your events, personnel announcements, and story ideas. **We are always looking for expert authors.**

Keeping the Planet and its' People Healthy

Health insurers embrace environmental stewardship

Health insurers are acknowledging that only a small part of health care happens at the doctor's office. According to AHIP research, insurance providers are taking a more inclusive view of health, including how to mitigate their environmental impact. Access to nutritious food and safe housing play a roll in a person's ability to maintain their health – along with the significant impact of sanitation, clean water and good air quality. The truth is that the clear link between physical and emotional well-being and the health of the environment disproportionately affects minority and underserved communities.

Read more: ahip.org/news/articles/how-we-keep-people-and-the-planet-healthy

EVENTS

Insurance Industry Charitable Foundation

(IICF) Inclusion in Insurance Forum

Advancing Ideas into Action. In person: New York, June 9 • Los Angeles, June 16 • Chicago, June 20 • Dallas, June 22.

Info: <https://inclusion.iicf.org>

National Association for Fixed Annuities (NAFA)

2022 Annuity Leadership Forum,

June 13-14, Washington, DC.

Info: nafa.com/events/annuity-leadership-forum/

OnRamp Insurance Conference: the leading conference for insurance innovation,

June 15, Minneapolis-St. Paul, MN. Info: onrampinsurance.com/conference

National African-American Insurance Association (NAAIA)

Juneteenth Event, June 16.

Info: naaia.org/calendar/2022/6/16/naaia-national-juneteenth-event

NAHU 2022 Annual Convention: The Power of Story,

June 25-28, Austin, Texas. Info: nahu.org/annual-convention

IEAHU, OCAHU & SDAHU Senior Summit,

Aug 23-25. Pechanga resort, Temecula, Calif.

Info: ieahu.net/senior-summit/

640%

Once Upon A Time There Was a Pandemic ... How children continue to suffer

Brightline has seen a 640% increase in demand for their services in behavioral health coaching. They specialize in helping parents find more intensive mental health resources for their children. Naomi Allen, founder and CEO of Brightline, shares an update on pediatric mental health and the increasing support employees need for their kids.

Enhanced Group Critical Illness Insurance from Aflac

Addresses serious mental illnesses and infectious diseases like COVID-19

Aflac's redesigned and enhanced Group Critical Illness product now gives employers the option to include coverage for infectious diseases, like the flu, pneumonia, human coronavirus and chronic conditions like diabetes. An additional mental illness rider is offered that covers serious mental illnesses, including bipolar disorder, post-traumatic stress disorder, substance use disorder, major depressive disorder and schizophrenia. This is in response to the changing needs of the workforce resulting from the pandemic.

VP Aflac Product Development and Management Kim Rudeen explained the reasoning behind the expanded offering, saying, "Employees bring their whole selves to work. That includes everything they're dealing with physically, mentally and financially, and the last two years have been especially challenging."

Read more: investors.aflac.com/press-releases/press-release-details/2022/Aflac-enhances-Group-Critical-Illness-Insurance-to-include-serious-mental-illnesses-and-infectious-diseases-like-COVID-19/

BenefitMall
NEXT GENERATION BROKER SERVICES

**DIGITAL
TECHNOLOGY
+ THE
HUMAN
FACTOR**

FASTEST, EASIEST, MOST TRUSTED.

BenefitMall.com | 800.350.0500

CAHIP 2022 Capitol Summit

A chance to meet with lawmakers

BY LINDA HUBBARD LALANDE

With California's heft, we super drive many of the nation's cultural trends – zoom zoom! – including how healthcare is delivered. So, one of California's premier insurance professional organizations, newly renamed California Agents & Health Insurance Professionals (CAHIP), has a HUGE role to play.

CAHIP works to help consumers – individuals, families and businesses – navigate the health insurance landscape. And since the Golden State has a burgeoning citizenry of 39

The focus was advocating for “what is good for consumers as well as the system as a whole.” The excellent speakers presented great information, from actual statistics to lifestyle changes that all could benefit from.

The gathered learned that 94% of Californians have health insurance, leaving only 6% uninsured. So, according to one of the presenters, “things are working well in our state – especially with the successful defeat of AB 1400 Single Payer. As we know, California policy often leads the way for the rest of the country and knowing single payer is still not palatable here is a relief to others across the country.”

Sue Wakamoto-Lee, CAHIP president-elect, noted in CAHIP's Statement May/June 2022, “A HUGE shout-out to our own VP of Legislation Dawn McFarland, for winning a Legislative Achievement Award for her effort leading CAHIP to assist in defeating single-payer legislation in the form of AB 1400. Great job, Dawn!

It was one of TWO Legislative Excellence Awards recently earned by California in Washington, D.C.

Presenter Justin Wallin of J. Wallin Opinion Research, was commissioned by CAHIP to do a survey of California voters.

We'll have a summary of that survey in an upcoming issue. The survey revealed that “Single Payer” is not wanted by a majority of Californians. It is not perceived as a feasible way to reach the increasingly popular concept of Universal Health Care for All.

Troy Underwood of Preventia Group gave an impassioned presentation on holistic wellness, stating that “we don't have a health care system, we have a sick care system.” Underwood is known as an industry disruptor and serial entrepreneur. According to his bio, “Underwood could sum up the nation's health insurance crisis with two

words: better diet.”

He talked of practical ways to combat poor health with a radical change to a plant-based diet that would combat obesity, heart disease, diabetes and much of what ails the American population. **We'll also be featuring Troy's approach in an**

upcoming issue.

Other important presentations included Calif. Assemblywoman Marie Waldron; Executive Director of Covered California Jessica Altman; and a NAHU leadership panel to give the national perspective, to name just a few.

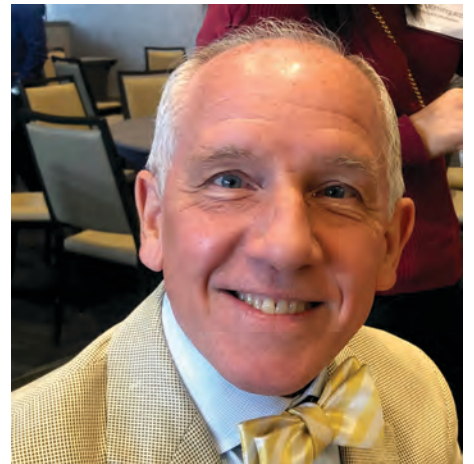
A fun and helpful skit to show members what to expect when meeting legislators face-to-face was a particular highlight. Amid much laughter, the audience saw firsthand the dos and don't's of legislative meeting etiquette – a great practice that will serve well when that exciting (and maybe a bit anxious) moment comes and folks are actually in front of a lawmaker!

So, stay tuned in and we'll be sharing more of the great information CAHIP sponsored for the 2022 Capitol Summit.

Fun Fact: The population of California is the largest in the U.S. and if California were a sovereign nation (2021), it would rank as the world's fifth largest economy — Amazing!



million and counting, that's a major undertaking. So, the CAHIP Capitol Summit in Sacramento May 9-11 was critical to get members educated on legislative issues and ready to meet face-to-face with California lawmakers.



CYBERSEC

**The Latest on Cyber-Attacks,
Ransomware and The Need
for Risk Assessment**

BY DOROTHY COCIU

It's been about a year since we were all on pins and needles about cyber-attacks and the news that Colonial Pipeline, JBS Foods and many others had been breached and their data held for ransom. This resulted in gas shortages and price hikes in the East and meat and food shortages everywhere.

SECURITY 2.0



There is no single federal law regulating cybersecurity or information security. We have a hodgepodge of state laws and minor federal laws, but no single protection source, as they do in the European Union and other nations.

This was followed by the 4th of July weekend, 2021 cyber-attack against the software company Kaseya, which targeted many small companies in up to 17 countries, (including the U.S., United Kingdom, South Africa, Canada, Argentina, Mexico, Kenya and Germany.) Cybersecurity experts believe the REvil gang, which is a major Russian-speaking ransomware syndicate, was behind the attack, targeting the software company by using its network-management package as a means to spread the ransomware broadly through cloud-service providers. Luckily, the software company was able to shut it down quickly, but not before significant damage was done.

When I wrote my last article on this topic, “Cyber Attacks Hit Home...The Next National Emergency? Valuable Cybersecurity Tools to Keep You Safe,” published in California Broker, August 2021 (www.calbroker.com/in-this-issue/cyber-attacks-hit-home-the-next-national-emergency), I detailed how these attacks happened and gave some advice on how to keep your organization safe, as did many others. Yet since then, we are still seeing the same issues popping up in the news on a far-too-regular basis. Breaches, hacks, cyber-attacks, ransomware.

Why does this keep happening? Because for many people, unless and until it happens to them, put off doing what they know they need to do — because it can’t happen to them, right? WRONG! It can, and it’s not a matter of “if” — it’s usually a matter of “when” it will happen to you. Your company — your data — in the hands of someone that shouldn’t have access to it. And then it’s too late. Your business is literally shut down. Your systems are basically dead. You’re scrambling to restore from backups, pay the ransom, notify the authorities and the victims, and in all cases, you’re retracing your work, putting in hundreds of hours (or thousands), or paying millions of dollars in crypto or other currencies, all to get your hands on what is already yours — your data!

How many times do you have to read about this stuff — hear about it on the news — listen to people who had it happen to them, before you actually do something to prevent it from happening to you? What’s the number? Ten? Thirty? A hundred? More?

Let’s do a little review first on what has happened since early 2021. Just in summary:

- **Colonial Pipeline:** Paid \$4.4 million. Fortunately 64 bitcoin (approximately \$2.3 million) was recovered by the U.S. government from a virtual wallet — the only known recovery to date of significance). It resulted in severe gas shortages, long lines and extremely high prices all over the East Coast.
- **JBS Foods:** Reportedly paid \$11 million due to the 2021 Memorial Day weekend attack, which caused severe meat shortages in an already pinched supply chain during the pandemic.
- **Kaseya Software:** The hack occurred affecting customers in approximately 17 countries.
- **Microsoft Exchange Server Breach:** In early 2021, attackers gained full access to user emails and passwords on affected servers, administrator privileges on the server, and access to connected devices on the same network. As of March, 2021, it was estimated that 250,000 servers fell victim to the attacks, including servers belonging to around 30,000 organizations in the U.S. and 7,000 servers in the United Kingdom, as well as the European Banking Authority, the Norwegian Parliament, and Chile’s Commission for the Financial Market (CMF).

Healthcare and insurance providers have of course been a huge target for cyber-attacks. We’ve heard about Anthem, Primera Blue Cross, Mass General, Cottage Health, UMass, Scripts and more, all falling victim to cyber criminals. It’s commonly felt that healthcare and medical information is susceptible to cyber-attacks because of the amount of highly sensitive data that they possess. Of course, the medical and insurance industries are subject to privacy and security laws such as HIPAA Security and HITECH, so there is a standard for protecting information. But as I said in my last article on this, there is no single federal law regulating cybersecurity or information security. We have a hodgepodge of state laws and minor federal laws, but no single protection source, as they do in the

European Union and other nations.

Mobile banking is among the latest victims. This includes Bank of America and Wells Fargo customers being scammed from outsiders using the mobile banking app Zelle to steal money from their accounts; and worse yet, the customers themselves allowed it to happen, because they thought they were talking to their banks. So, instead of stopping it, they basically allowed the Zelle hackers to take money directly from their accounts.

Another very scary security scenario, in my opinion, is everyone's use of QR Codes. They've become all the rage — but they are also susceptible to hacking, which I will discuss further later in this article.

And let's not forget Mobile Ticketing and the requirement of season ticket holders and individual game purchasers to download their team's league app. Users do this without thinking twice and don't question the permissions they are granting, which can be a security nightmare.

So, for anyone reading this, it's not over. That storm I talked about last summer and fall in my article referenced earlier has not passed. If we thought we were in the eye of that storm then, I hate to be the bearer of bad news, but it's more like a season of continuing storms with no clear skies ahead. The trend for more cyber-attacks and ransomware is continuing, because most of us are allowing the bad guys to keep doing it!

As long as we still have that Weakest Link — fallible human beings in charge — we will always have risks. We need to learn how to manage those risks, now and in the long-run. Until we do, we will continue to hear news reports on breaches and ransomware, and companies will continue to be at risk.

I will provide you with more detail on these recent breaches, hacks, scams and the current risks you should be aware of below.

Microsoft Breach by Lapsus\$ Hacker Group, March 2022

Just this past March, Microsoft announced it was breached by Lapsus\$ Hacker Group. News reports said that a screenshot was taken indicating that Bing, Cortana and other projects had been compromised in this breach.

As I often do, I looked to my HIPAA Security/HITECH and IT Services and Security partners, Aditi Group, to offer some insight from an IT or technical perspective as to what happened. What should Microsoft users be worried about? Or what do they need to do to protect themselves? I was able to gain some additional insight to share with you in my conversations with Ted Flittner and Ted Mayeshiba, principles of Aditi Group.

"This group has also just successfully attacked T-Mobile and a growing list of big-name companies," noted Flittner. "What happened with Microsoft is that hackers allegedly stole portions of source code for the search service Bing, and the navigation for Bing Maps and Cortana (Microsoft's answer to Siri). Microsoft's public statement is that obtaining portions of source code does not put the general public at risk."

Flittner continued, "In truth, knowing the code can increase risk by allowing hackers to scrutinize it and find weaknesses that Microsoft hasn't found or fixed. That said,

since these services (Bing, Maps, Cortana) don't require user login info, there probably is not a risk."

Block (formerly Square) Breach, April 2022

More recently, Block (formerly Square) acknowledged that its cash app had been breached by a former employee in December, 2021. It's reported that over 8 million customers were affected. The breach included customer names, brokerage account numbers, portfolio information and stock trading activity. They are claiming that no other personally identifiable information or account credentials were leaked in the incident. What is the danger of this sort of breach? Again, I went to my tech experts.

"This is a straightforward case of a former employee still able to log into Block's cash app system and download user reports," stated Flittner. "These are the same reports the employee was authorized to view while still working there. Even if no personally identifiable info was accessed, the data that was downloaded is PRIVATE info that people only want to share with their tax accountant or investment advisor. That sort of info helps criminals pick which people to target in phishing scams. Think Frank Abagnale, Jr., the real-life person played by Leonardo De Caprio in the film "Catch Me If You Can." Frank just needed some info about people to pretend to be them — and easily scam people for money."

T-Mobile Breach, April 2022

I also discussed the recent T-Mobile attack by Lapsus\$, since it was the same hacker group as the Microsoft hack, with Flittner. I asked him to let us know what happened and how it happened.

"The T-Mobile attack by Lapsus\$ in April 2022 did not breach customer data directly," he explained. "T-Mobile has had its share of that, including a breach of 47 million customers' personal data in 2021. This Lapsus\$ attack involved BUYING T-Mobile employee VPN (virtual private network) login info. This was purchased on the dark web with the goal of escalating and accessing T-Mobile's account management system and ultimately allowing hackers to 'SIM swap.' That's when you tell the phone company that the phone number is now tied to a different SIM card. This lets someone hijack your cell phone. And if your cell phone is used for account verification — text messages for example, the hacker now can bypass multi factor authentication."

Flittner continued, "Though hackers didn't get far enough this time, it highlights the problem of phone numbers being hacked. And why we recommend using multi factor authentication with a hardware key — like Yubico."

Are banking apps safe?

The world of banking has evolved to the now "must have" banking apps on your mobile devices. Banks need to draw new customers, and many of them are young and tech-savvy. They've literally grown up on the technology some of us are still trying to adapt to in our everyday lives.

Zelle is used by many banks in the U.S. today to easily transfer and send money. These banks include Bank of America, Capitol One, Wells Fargo, U.S. Bank, JP Morgan Chase and PNC Bank. Of course, Apple also offers their Apple Bank mobile app, and there are many more. But are

they safe?

I briefly described earlier the recent scams using Zelle that cost customers of Bank of America and Wells Fargo hundreds to thousands of dollars. Scammers spoofed the banks' phone numbers and the customers were sent text messages, followed by a phone call, which informed them of an attempt to transfer funds. As a "preventive measure" the scammers gave instructions to the customers which instead sent their funds off to the scammers. Sadly, the banks are not actually obligated to replace the money if their customers authorized the money transfers, which in these instances happened.

So, how do we keep our money safe if we're using banking apps on our mobile devices? Here's Aditi Group, to give more information from the tech side.

"These banking scammers are really using age-old tactics: pretending to be someone they're not," Flittner relayed. "The callers use false Caller ID for the phone call and text messages to innocent bank customers. They SAY they're from Wells Fargo or BoA or another of the most common banks. Some people have been fooled into divulging their account credentials 'to avoid attempted fraud.' And in the process they ALLOW the fraud."

Flittner continued, "This is not a failure by the application. This is a failure to understand how a fraud investigation really works. The financial institution doesn't ask for your login credentials. But when you call them, they ask you to verify who you are — name, birthdate, address, last 4 numbers of your Social Security number. **We all need to be sure WHO we're talking to on the other end of the line.** Is it the BANK or a SCAMMER? We recommend always calling the bank back. Check the number they give you and see if it matches the phone number on the back of your credit card or the bank. If not, call the phone number you KNOW for your bank and ask about it." That is something that we've encouraged people to do for several years.

"Banking apps are as safe as using a web browser normally," continued Flittner. "Potential security problems include logging into apps when others can see you, or working on public wifi, where hackers may have obtained access to your phone or computer. Other problems are the general ones that apply whether it's a mobile app or web browser on a computer, like using weak passwords or leaving your password around for others to find. And with phones, leaving them unattended without a strong password to keep others from doing bad things while you're not looking."

The risks of using QR codes

QR Codes are all the rage. If you don't have one and you're trying to advertise something, you feel like if you don't have one, you'll be left behind and lose out to your competitors. And now it's not just advertising. QR codes can be found everywhere. The problem is, they too can be compromised. Thieves and bad actors have begun placing their own QR codes over the originals and sending phones to unsafe sites where again, bad things can happen.

Keep in mind, a QR code uses the phone's camera — therefore it needs access to your camera, and will often ask for (and people automatically give) permission to view all of your files and photos on your device. Wait, what? All of

your photos and all of your files? Are your company files in dropbox, which you can access from your phone? Are your emails from your customers, or their private information such as their names, phone numbers, account numbers, maybe credit card numbers in those files on your phone? If so, do you want every entity that you scan a QR code for to have all of that information? If not, you might want to think twice about using QR codes without scrutinizing them.

"Look before you leap," Flittner emphasized. "Does the QR code look legit or is it like sticker graffiti on a traffic light pole? If it looks like someone pasted a sticker on the original — STOP." It sounds simple, but many people just don't stop to take that second look, and that is a real problem.

"If you do scan the code, look at the website address (URL) that it shows before agreeing to load the page. Only use the QR code read apps or camera apps that let you choose to visit the website or not, instead of having it load automatically," continued Flittner. "Once it loads, look at the website to be more certain it's real before you enter any personal data, credit card or sensitive info."

Mobile ticketing apps

Whether you're a concert-goer or a sports fan, or anything in-between, it's likely your event is now using Mobile Ticketing only. The problem with mobile ticketing apps is that they can be unsafe because people don't always look at the permissions they are granting to the app when using it. Most people automatically click yes to accept the terms without looking further or questioning the app's intentions.

My company has season tickets for the Anaheim Ducks (NHL) and the LA Rams (NFL), and both have mobile ticketing. But me being me, and being worried about the dangers of mobile apps, I always ask the team if I can get paper tickets. Yes, it's old-fashioned, but much safer. Sometimes if you ask, there is no charge to get paper tickets. Sometimes you have to pay a paper ticket fee, but to me, it's worth it. Why? What's so scary about these apps?

I've seen the apps asking for permission to access your files, your photos, and get this, your network access. So, before you start clicking okay for all of these permissions you're granting, slow down. Figure out how to see all of the permission requests and how to say no to what they do not need and what you do not want to give them access to. If you're not sure, contact an IT or security expert.

If you are a big user of ticket apps and such, another option is to have a second phone — one for business and one for things like mobile ticketing apps. For the latter, don't store anything on the second phone. Use it only for those concerts or sporting events. (And yes, it can be expensive to have two phones. See if a very limited plan can be used for the latter).

Crypto currency

Crypto currency is the latest rage. Everyone wants it. Even buildings now display their names, but no one is regulating it. In January 2022, it was reported that \$30 million was stolen in the Crypto.com breach (\$18 million in bitcoin and \$15 million in Ethereum, as well as other cryptocurrencies). I asked Aditi Group if they could tell us more about crypto currency and the dangers of using it. If people are buying it

and trading with it, is there anything that can be done to protect them?

“There are probably THOUSANDS of crypto currency offerings now,” stated Flittner. “It takes very little to create one and make it public. And without regulation and with investor frenzy over potential profits to be made, it’s easy to get caught up in emotion and skip due diligence. Simply from an investment perspective, crypto investing is gambling. It can pay off for you or wipe out your savings.

“From a security perspective, it requires smart and strong password management,” he warned. “The main path of breach is someone getting your login and password to your crypto wallet. Guard those passwords. Make them as strong as possible.”

Flittner continued, “Crypto.com, which is a crypto trading platform, was breached by hackers and discovered this January. Hackers were able to bypass the 2-factor authentication for user accounts and 483 accounts were accessed. \$30 million in bitcoin and ethereum (crypto coin) was stolen. Crypto.com reimbursed the user accounts and stopped other attempted transfers. They have since announced stronger ‘multi-factor’ authentication coming this year,” Flittner explained.

“Part of the risk with crypto is once it’s stolen, you may have no recourse,” continued Flittner. “Crypto.com is rolling out a new Worldwide Account Protection Program that can insure your account up to \$250,000 – if you meet certain conditions.” So if you’re thinking of investing in crypto currency, be sure you do your homework and put in the necessary security protocols before you invest.

How do we protect ourselves and our companies?

So, how do we protect ourselves from these common threats? As a privacy and security consultant and trainer, my first instruction is always to **DO A RISK ASSESSMENT**. Figure out where your risks are so you can mitigate them. You need to know where you are before you can move forward with a security plan.

“This is all about being aware of danger before it strikes,” stated Flittner. “And prepare to reduce risk and recover faster if it does.”

The need for risk assessments – an ongoing security tool

Every article I write about this topic and every training I do includes my preaching to you all about the need to do risk assessments. This means you must look at every device, every tool, every router, your network, and everything else to determine where the risks are, and figure out how to mitigate those risks.

According to Flittner, “In basic terms, this is a comprehensive review of you or your business to consider what risks you may face (stolen computer, ransomware attack, even physical break-in); and what inherent vulnerabilities you have (staff bringing their own computers, working from home, running out-of-date software). What’s the likelihood of each type of problem actually happening, and the impact if they do? Then decide which items are really critical to address, which are less serious, and on down. Sometimes we conclude that chances are LOW that a problem happens, but the IMPACT would be catastrophic, so we take steps to avoid or easily recover (think life insurance).”

Flittner continued, “The result should be ACTION to address the dangers. HIPAA and HITECH require it for businesses that fall under HIPAA. And it’s often mentioned by the federal investigators in HIPAA violations as missing or lacking.”

Identify technical vulnerabilities to include in risk analysis.

In their March 17, 2022 OCR Cybersecurity Newsletter “Defending Against Common Cyber Attacks,” they recommend:

- Subscribe to Cybersecurity and Infrastructure Security Agency (CISA) alerts (<https://us-cert.cisa.gov/ncas/alerts>) and bulletins (<https://us-cert.cisa.gov/ncas/bulletins>)
- Subscribe to alerts from the HHS Health Sector Cybersecurity Coordination Center (HC3) (<https://www.hhs.gov/about/agencies/asa/ocio/hc3/contact/index.html>)
- Participate in an information sharing and analysis center (ISAC) or

This is not a failure by the application. This is a failure to understand how a fraud investigation really works. The financial institution doesn't ask for your login credentials. But when you call them, they ask you to verify who you are – name, birthdate, address, last 4 numbers of your Social Security number. We all need to be sure WHO we're talking to on the other end of the line. Is it the BANK or a SCAMMER?

Before you start clicking 'okay' for all of these permissions you're granting, slow down. Figure out how to see all of the permission requests and how to say no to what they do not need and what you do not want to give them access to. If you're not sure, contact an IT or security expert.

information sharing and analysis organization (ISAO)

- Implement a vulnerability management program that includes using a vulnerability scanner to detect vulnerabilities such as obsolete software and missing patches; and
- Periodically conduct penetration tests to identify weaknesses that could be exploited by an attacker.

According to OCR, regulated entities, should not rely on only ONE of the above techniques, but rather should consider a combination of approaches to properly identify technical vulnerabilities within their enterprise. Once identified, assessed, and prioritized, appropriate measures need to be implemented to mitigate these vulnerabilities (e.g., apply patches, harden systems, retire equipment).

How often should a risk assessment be done? “We recommend a yearly review or when major changes happen with the business,” Flittner noted.

Who should be involved in a risk assessment?

Is it just IT? “Risks involve the whole team,” Flittner said. “Key supporters of risk assessments should include executives, especially financial leadership. But really, everyone in the business should be involved in some way.”

What are some of the areas in an organization that need to be looked at in a risk assessment?

“Everywhere that sensitive info moves throughout your business,” replied Flittner. “This could just be one department like Human Resources, or it could affect everyone.”

What sort of questions, tasks, need to be included in a risk assessment?

Ted Mayeshiba of Aditi Group responded as follows, “Do a physical inventory. What devices hold sensitive data (Protected Health Information [PHI] in HIPAA terminology). Important questions include: ‘Where does the data reside? What’s in ‘the cloud’ with third party companies? Who should access the sensitive info? And how do you control access? Is there a business associate (BA) agreement in place? Does the third party company have access to the data? All of these should be considered and discussed within your organization.”

We always recommend that a risk assessment be done by an independent third party.

Why? According to Flittner, “There are three main reasons: first — it’s not the main job of employees, so it rarely gets priority; second — outside eyes tend to notice problems that people who see the process every day can miss (can’t see the forest through the trees); and third — employees sometimes are reticent to admit to weaknesses in the process.”

I asked Flittner what message he would share with every business owner, large or small, related to risk assessments and their importance in protecting their data? Flittner replied, “Know before it’s too late. BE PREPARED. As a former Boy Scout, I learned to live by that motto long ago. Security is always evolving and where you didn’t think you had risk in the past may be totally different today. And the cost of problems like data breaches and ransomware are much higher than the cost of prevention.”

Weak cybersecurity practices

It is well known that a regulated entity that has weak cybersecurity practices makes itself an attractive soft target for hackers and cyber criminals. Weak authentication requirements are frequent targets of successful cyber-attacks. Over 80% of breaches due to hacking involved compromised or brute-forced credentials, according to OCR. (Verizon. 2020 Data Breach Investigations Report 2020, p. 19 <https://enterprise.verizon.com/resources/reports/2020/2020-data-breach-investigations-report.pdf>.)

Weak password rules and single factor authentication are among the practices that can contribute to successful attacks.

Once inside an organization, if the entity has weak access controls, this can further contribute to an attacker's ability to compromise systems by accessing privileged accounts, moving to multiple computer systems, deploying malicious software, and exfiltrating sensitive data.

HIPAA rules state that regulated entities are required to verify that persons or entities seeking access to ePHI are who they claim to be by implementing authentication processes. (See 45 CFR 164.312(d): Standard: Person or Entity Authentication.)

A regulated entity's risk analysis should guide its implementation of appropriate authentication solutions to reduce the risk of unauthorized access to ePHI. For example, authenticating users that access a regulated entity's systems remotely (e.g., working from home) may present a higher level of risk to a regulated entity's ePHI than users logging into their desktop computer at work. To appropriately reduce the higher level of risk of remote access, a regulated entity may consider implementing stronger authentication solutions, such as multi-factor authentication.

According to OCR's March 17 newsletter, implementing access controls that restrict access to ePHI to only those requiring such access is also a requirement of the HIPAA Security Rule. (See 45 CFR 164.312(a)(1): Standard: Access Control.) Here, too, the risk analysis should guide the implementation of appropriate access controls. For example, a regulated entity may determine that because its privileged accounts (e.g., administrator, root) have access that supersedes other access controls (e.g., role- or user-based access) – and thus can access ePHI – the privileged accounts present a higher risk of unauthorized access to ePHI than non-privileged accounts. Not only could privileged accounts supersede access restrictions, they could also delete ePHI or even alter or delete hardware or software configurations, rendering devices inoperable.

To reduce the risk of unauthorized access to privileged accounts, the regulated entity could decide that a privileged access management (PAM) system is reasonable and appropriate to implement. A PAM system is a solution to secure, manage, control and audit access to and use of privileged accounts and/or functions for an organization's infrastructure. A PAM solution gives organizations control and insight into how its privileged accounts are used within its environment and thus can help detect and prevent the misuse of privileged accounts.

Regulated entities should periodically examine the strength and effectiveness of their cybersecurity practices and increase or add security controls to reduce risk as appropriate.

Regulated entities are required to periodically review and modify implemented security measures to ensure such measures continue to protect ePHI. (See 45 CFR 164.306(e): Maintenance.) Further, regulated entities are required to conduct periodic technical and non-technical evaluations of implemented security safeguards in response to environmental or operational changes affecting the security of ePHI. This is to ensure continued protection of ePHI and compliance with the Security Rule. (See 45 CFR 164.308(a)(8): Standard: Evaluation.)

Examples of environmental or operational changes could include: the implementation of new technology, identification

of new threats to ePHI, and organizational changes such as a merger or acquisition. But even if you're not a HIPAA Covered Entity, these practices should apply to any organization due to the many other state and federal privacy and security rules, and as a matter of overall good business practice to keep your organization's data safe.

New federal guidance on defending against common cyber-attacks

In the past few months, both the IRS and HHS's Office of Civil Rights have issued guidance and newsletters for HIPAA Covered Entities on keeping you safe against common cyber threats. I'll highlight some of the most important tips. I would suggest you read the HHS Office for Civil Rights In Action March 17, 2022 OCR Cybersecurity Newsletter "Defending Against Common Cyber Attacks," which I mentioned earlier. It can be found at: www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-first-quarter-2022/index.html.


In addition, the IRS published several releases in February 2022, to protect taxpayers from scams and fraudulent activity (www.irs.gov/newsroom/irs-warning-scammers-work-year-round-stay-vigilant), as well as announcing a transition away from the use of third-party verification involving facial recognition (www.irs.gov/newsroom/irs-announces-transition-away-from-use-of-third-party-verification-involving-facial-recognition).

I will summarize some of the more important items discussed in these publications and provide additional commentary. I also want to point out that since we don't have a single national entity regulating all forms of electronic and cybersecurity, even if you're not a covered entity under HIPAA rules, the HIPAA Security and HITECH rules are very effective in protecting your organization from all types of electronic and cybersecurity threats. Simply, it's all we have, for the most part, so use those rules to your advantage.

Phishing, spear phishing and whaling

As discussed in my last article, one of the most common attack vectors is phishing. This is a type of cyber-attack that is used to trick individuals into divulging sensitive information via electronic communications, such as by email, or by impersonating a trustworthy source. According to HHS, a recent report noted that 42% of ransomware attacks in Q2 of 2021 involved phishing.

If you're subject to HIPAA Security and HITECH (meaning you are a HIPAA Covered Entity, such as a sponsor of a health plan, an insurance company or a provider of health care services) your workforce members should understand that they have an important role in protecting the ePHI of their organization from cyber-attacks, according to OCR. Part of that role involves being able to detect and take appropriate actions if someone in your organization encounters a suspicious email. The problem is, if they are not trained to detect suspicious emails, they will go unnoticed, and bad things generally tend to happen as a result. These regulated entities should train their workforce (there is that word again – train) to recognize phishing attacks and implement a protocol on what to do when such an attack or suspected attack occurs.



Every article I write about this topic and every training I do includes my preaching to you all about the need to do Risk Assessments. This means you must look at every device, every tool, every router, your network, and everything else to determine where the risks are, and figure out how to mitigate those risks.

Do you have such protocols in place in your organization?

Do your employees know who they are supposed to report suspicious emails to in your organization? Is anyone assigned to be that person or department?

Mayeshiba shared, “In the latest Office of Civil Rights (OCR) newsletter, the government tipped their hand as to the raising of the threshold of ‘reasonable efforts’ for evaluating companies ‘best efforts’ defending against common cyber-attacks. There is a new and repeated reference to ‘penetration attacks’ as a best practice which should be adopted by companies.”

Mayeshiba continued, “Penetration testing is usually a third party outside attack on your company’s network by ‘friendly’ forces that test weaknesses in your network. This is really nothing new. This is routinely done by Fortune 500 firms. However, it is the first time that we’ve witnessed this idea put forth in a regular OCR Cybersecurity newsletter. Of particular interest was the reference to tie cybersecurity training programs with a follow up with friendly ‘phishing’, ‘spear phishing’ and ‘whaling’ attacks to test the effectiveness of the training. As attacks become more frequent and target even ‘small’ firms, it is becoming increasingly urgent to tighten cybersecurity for all firms.”

According to Mayeshiba, “Phishing is a type of social engineering attack commonly used to steal user data including login credentials or other financial data. It commonly occurs when an attacker, masquerading as a trusted entity, dupes a victim into revealing sensitive information by opening an email, link or text message. Spear phishing is similar to phishing, but the attack includes specific information unique to the individual being attacked, thereby increasing the likelihood of the victim opening the email, link or text message.”

Another term not mentioned in the OCR Newsletter is ‘whaling’. Mayeshiba defines this as “similar to phishing, but the attack is specific to executives (C-suite) or to others where the bad actor masquerades as the executive to coerce a trusted employee to divulge sensitive information.”

According to the HIPAA Security Rule, regulated entities are required to implement awareness and training programs to all its workforce members. Such programs should be an ongoing and evolving process, so that it changes as new threats develop. Your management personnel should also be participating in training — I’ve seen far too often that they want their employees to be trained, but the executives fail to go through training themselves. Then when they are targeted, which they often are because they have access to a generally a higher amount of ePHI in phishing email attacks, they don’t follow protocols. They are often the reason for such schemes resulting in bad things happening.

The key to an effective security training program is repetition and periodic security reminders. In fact, the Security Rule includes an addressable provision for such reminders. Are you doing this within your organization?

OCR recommends that covered entities should, for example, send simulated phishing emails to your workforce members to gauge the effectiveness of their security awareness and training program and offer additional, targeted training where necessary. An educated workforce can be an effective first line of defense and an integral part of a regulated entity’s strategy to defend, mitigate and prevent cyber-attacks.

In my opinion, the worst type of training you can provide is a canned, “check-the-box” training consisting of a few simple presentation slides. It’s best to think of interesting, innovative ways to engage your workforce to understand the risks and prevent cyber-attacks.

OCR suggests that regulated entities mitigate the risk of phishing attacks by implementing anti-phishing technologies. This could mean examining and verifying that received emails do not originate from known malicious sites. If an email is suspected of being a threat, it can be blocked and appropriate personnel can be notified to step in and deal with the threat head-on. Other approaches, according to OCR, involve scanning web links or attachments included in the emails for potential threats and removing them if a threat is detected. Newer techniques leverage machine learning or behavioral analysis to detect potential threats and block them as appropriate.

The key is developing and implementing “policies and procedures to protect ePHI from improper alteration or destruction.” It’s important to note that the Security Rule requires regulated entities to assess and reduce risks and vulnerabilities to the availability of ePHI, as well as confidentiality and integrity.

Anti-phishing technologies can impede or deny the introduction of malware that may attempt to improperly alter, destroy, or block authorized access to ePHI (for example, ransomware), and thus can be a helpful tool to preserve the integrity and availability of ePHI, according to OCR.

It is always advisable to combine an educated, engaged workforce with technical solutions in order to achieve the best opportunity to reduce or prevent phishing attacks.

Exploiting known vulnerabilities

I think most of you know and understand that hackers can penetrate an entity’s network and gain access to ePHI or other sensitive data by exploiting known vulnerabilities, where they are publicly known to exist. The National Institute of Standards and Technology (NIST) maintains the National Vulnerability Database (NVD), which provides information about known vulnerabilities. Exploitable vulnerabilities can exist in many parts of your information technology infrastructure, such as on your server, your desktop, mobile device operating systems, applications, databases, your web software, your router, your firewalls, and other device firmware. Often known vulnerabilities can be mitigated by applying vendor patches or upgrading to a newer version. If a patch or upgrade isn’t available from the vendor, they may suggest actions you can take to mitigate a newly discovered vulnerability. These could include modifications of configuration files or disabling affected services.

It’s important to remember that older applications or devices may no longer be supported with patches for new vulnerabilities. So, you will need to take appropriate action if a newly discovered vulnerability affects older applications or devices. If an obsolete and unsupported system cannot be upgraded or replaced, then additional safeguards must be implemented or existing safeguards enhanced to mitigate the known vulnerabilities until an upgrade or replacement can occur. This may involve increasing access restrictions, removing or restricting the old device from network access, or disabling unnecessary features or services.

The bottom line is, you need to do a risk analysis to determine these potential risks and vulnerabilities. Not once, but often and on an ongoing basis.


Read, sink in, repeat — the need for continued training

Although I discussed this in detail in my first article, I do want to touch on it again. It’s imperative that employers take the time to train their employees on the electronic risks that are out there. If you don’t, it only takes one wrong click on an emailed link to download malware, worms or other things that can bring your systems to a screeching halt. As Flittner stated in that article, “Know company policies and why it matters to follow them. The key topic these days is email diligence. Don’t click on email links or download files that you don’t really know. Slow down and take time to scrutinize. Teach people how to recognize fakes and legitimate

messages. Train people on how to react if malware, ransom or phishing attempts succeed. Who should they call and what should they do next? That seems to be one of the glaring missing pieces in most employers’ privacy policies.”

Bottom line, train now and train often. You can never train enough. Things change, and so should your training. Keep up to date and keep up with the latest threats.

Same message, different result?

Although to some extent I am sharing with you the same message as my prior article from 2021, I’m hoping for, someday soon, a different result. We don’t need to keep repeating the same mistakes and putting off until tomorrow something that should have been done yesterday. The only way to have a different result, a better result, with less hacks, less cyber-attacks, is to do what you know you need to do. **Do a risk assessment.** See where you are and where you want to be and develop policies and procedures to help you meet your goals. And don’t forget to train your employees regularly and often, keeping up-to-date with the latest threats. I’d like to think that perhaps someday soon I won’t have to keep writing these articles every year. So, let’s work on a different result, please! 

Author’s Note: I’d like to thank Ted Flittner and Ted Mayeshiba of Aditi Group for their assistance with this article. Reach them at AditiGroup.com, or by email at ted.flittner@aditigroup.com or ted.mayeshiba@aditigroup.com.

Advanced Benefit Consulting & Aditi Group offer privacy & security training, consultation and implementation system assistance, as well as Risk Assessment services on an ongoing basis.



DOROTHY COCIU is the president of Advanced Benefit Consulting, Anaheim, CA, and the current VP of Communications, California Agents & Health Insurance Professionals (CAHIP) 2021-2022.

Contact:
dmcociu@advancedbenefitconsulting.com
714 693-9754 x 3.

References & Sources:

HHS Office of Civil Rights March 17, 2022 Newsletter, “OCR Cybersecurity Newsletter: Defending Against Common Cyber Attacks.”

IRS publications February, 2022:

- www.irs.gov/newsroom/irs-warning-scammers-work-year-round-stay-vigilant)
- www.irs.gov/newsroom/irs-announces-transition-away-from-use-of-third-party-verification-involving-facial-recognition.
- Plus sources referenced in the article.



Emma got a phone call from a nice gentleman saying her cardiologist had ordered a cardiac genetic test kit for her. “Oh, well that’s a surprise,” she said. But the man assured her that her doctor wanted to screen for her risk of heart disease. As the caller said he had her doctor’s name and her Medicare number, Emma relaxed and remarked, “Well, this is mighty kind of my doctor.” The gentleman agreed, saying he was happy to send the kit her way, but needed her to “verify” her doctor’s name and her Medicare number to make sure he was indeed talking to the right Emma.

It seemed logical enough; Emma shared her information, and that was that.

Fast forward a couple weeks and Emma received her genetic testing kit in the mail, spoke with someone who guided her step by step on how to complete it, and sent it back completed.

When reviewing her Medicare Summary Notice (MSN) a couple weeks later, a document Medicare sends out every three months that reviews any Medicare Part A and/or B covered services used, Emma noticed some excessively expensive charges related to genetic testing. The company billed Medicare \$7,485.87 for the tests and Medicare paid \$5,963.38!

Yet it wasn’t until the next day when Emma attended one of our California Senior Medicare Patrol (SMP) presentations on Medicare fraud, that Emma knew she’d been scammed.

The presentation alerted seniors about rampant genetic testing fraud, and Emma reported it to SMP right away. Our team advised her about the importance of guarding her Medicare card, how she can prevent further fraudulent charges from being billed, and explained what we do with her case. California SMP assured Emma that her case was referred on to the Office of Inspector General and the Center for Medicare and Medicaid Services’ (CMS) San Francisco Regional Office for investigation.

This is just one of thousands of cases of genetic testing fraud happening around California and nationwide. Last year alone, one in every four cases reported to our California Senior Medicare Patrol (SMP) was a genetic testing scam.

What is genetic testing fraud?

Simply put, genetic testing fraud occurs when Medicare is billed for a test or screening that was not medically necessary and/or was not ordered by a beneficiary’s treating physician.

Across the nation, genetic testing company representatives are offering

“free” genetic tests to any and all Medicare beneficiaries. Yet, these tests are NOT medically necessary and are NOT ordered by the person’s physician. (Medicare only covers them when they are medically necessary and ordered by the beneficiary’s doctor).

The tests are advertised as DNA screenings, cancer screenings, dementia and Parkinson’s screenings, pharmacogenetics (medication metabolism), heart disease screening, hereditary testing and more. The representatives/fraudsters go to senior centers, senior housing, health fairs, and even parking lots to convince people to let them take a cheek swab for testing. They advertise on TV and online via email, Facebook and Craigslist, to name a few. Sometimes they offer ice cream, pizza, or \$100 gift cards. And other times they even claim to be calling from Medicare. They promise that the results will help recipients avoid diseases or find the right medications. All they ask for in return is the person’s Medicare number.

Does it sound too good to be true? That’s because it is. It’s a scam.

How much does genetic testing fraud cost?

This scam costs Medicare a massive amount of money, draining the system

of funds needed to pay for people's care. Medicare on average pays \$6,000 to \$9,000 for each of these tests, and sometimes as much as \$25,000 for a single beneficiary, according to the Office of Inspector General at the Department of Health and Human Services. A few years ago, one 72 year-old Vietnam veteran even reported that \$32,212.86 was billed to his Medicare supplement insurance plan! This was for a DNA test he was persuaded to get at an event at his local senior center.

With Medicare paying so much money for these tests, these companies often pay generous kickbacks to doctors who agree to order DNA tests for patients without ever treating them. The front-line recruiters who solicit the tests might work directly for a lab, or as independent contractors who divide revenue with a laboratory in exchange for bringing in extra business. And the money to be made is big.

One Florida doctor charged in federal court for his role in a fraud scheme to order DNA tests for patients in four different states confessed to being paid \$5,000 per month to approve these tests. And this is without ever speaking to any of the patients involved.

Examples of fraudsters abound, as do the cases of victims to this fraud. One fellow, as reported in Kaiser Health News, was a 71-year-old retired police detective who had submitted a DNA test at a health fair. They were advertising "free" cancer screenings covered by Medicare, and as cancer had run in his family, he thought it would be good to get. Three weeks later, he saw the same people knocking on doors at his RV park and testing his wife, friends, and neighbors. As a retired detective, he was familiar with the costs of DNA tests, so was shocked when he checked his Medicare Summary Notice to see Medicare billed \$10,410 for his tests! He also never received his results until he called and asked for a copy.

When the results arrived, they listed his results as "uncertain" and "a bunch of gobbledygook that makes no sense to anybody who's not in the medical field," he said. He reported this fraud.

Risks to beneficiaries

Not only does Medicare lose large amounts of funds to these scams, it is also dangerous for beneficiaries.

Their DNA information is stolen, and their identity and medical identity is compromised. This can lead to their Medicare numbers being used to order services and items they never receive. This can mean that if (or when) a beneficiary does need a service or item, such as a wheelchair, if their account shows that Medicare already paid for one, they would be blocked from receiving the wheelchair they need.

Also, while Medicare usually foots the bill on these tests, sometimes it doesn't and then the beneficiary gets stuck with an expensive \$7,000 to \$10,000 bill. One man in Southern California who reported his case of genetic testing fraud to our SMP, said when he got his kit in the mail, he remembered seeing and signing a slip of paper that said he agreed to pay for the test if Medicare denied it.

Another woman who called a company in response to an online ad for a genetic testing kit, now receives robocalls off the hook. While she didn't give them her Medicare number, the scammers now have her cell phone number which they've shared with or sold to numerous third parties.

How to avoid genetic testing scams


With so much at stake in draining Medicare funds, compromising one's medical identity, having stolen DNA information, having one's Medicare number compromised and more, it's important to avoid this scam. Here are some helpful tips to do just that:

- Refuse to give out your personal information or accept screening services, including a cheek swab, from someone at a community event, local fair, farmer's market, parking lot, mall, senior center, home show, church-sponsored wellness event, and/or any other large event.
- Go to your own doctor to assess your condition, not a doctor on the phone you've never met from a company you don't know.
- Always read your Medicare Summary Notice (MSN) or Explanation of Benefits (EOB). The words "gene analysis" or "molecular pathology" as service codes may indicate questionable genetic testing.
- Refuse the delivery of any genetic testing kit that was not ordered by your physician.
- Be suspicious of anyone who

offers free genetic testing and then requests your Medicare number. If your personal information is compromised, it may be used in other fraud schemes.

- Contact our California SMP for help. SMPs across the nation empower and assist Medicare beneficiaries, their families, and caregivers to prevent, detect, and report health care fraud, errors, and abuse.

If you, a loved one or a client you know come across such scams, please report them to our California SMP at 1-855-613-7080.

The California SMP works to provide you, your clients and loved ones with the information they need to PROTECT themselves from Medicare fraud, errors, and abuse; DETECT potential fraud, errors and abuse; and REPORT their concerns. We educate and empower Medicare beneficiaries in the fight against healthcare fraud. Our SMP can help with questions, concerns, or complaints about potential fraud and abuse issues. We also provide information and educational presentations. 

Contact us at 1-855-613-7080.

Together we can help stop this genetic testing fraud and other Medicare fraud.



KAREN JOY FLETCHER, MPH, has over 20 years of experience in Medicare training, education and advocacy and has served as California Health Advocates (CHA's) publications

consultant since 2004. She is the primary researcher, writer and editor of CHA's website content, including CHA's newsletter and blog. She also develops and revises key educational materials, spearheads CHA's social media and chairs the Senior Medicare Patrol (SMP) Media Team and SMP superheroes skit team.

In addition to her Medicare advocacy work, Fletcher teaches Earthgym and Qigong at schools, conferences, festivals and retreat centers around the country and abroad, and co-leads Qigong & Wilderness retreat trips in China. She also enjoys ample nature and family time in the Cascadian forests and mountains.

www.karenjoyfletcher.com



Insurers Required to Offer COVID-19 Tests At No Cost To Plan Members

Members of private insurance plans are allowed eight over the counter tests per calendar month

BY MICHAEL GIUSTI

Six months into the Biden administration's mandate that private insurers cover at-home COVID-19 rapid tests, things are going a lot smoother than they did out of the gate.

Most insurers have since worked out the details, and Medicare is now getting into the act, covering at-home tests for Part B and Advantage members. Following an initial surge in demand, COVID tests are also readily available on pharmacy counters and through mail order providers.

How did we get here?

In January, the Biden administration offered up a potentially powerful tool for combatting the pandemic — no-cost-to-consumer over-the-counter tests for people with private insurance.

The mandate for insurers to cover over-the-counter tests came down from the White House, along with the Department of Labor, Health and Human Services, and the Department of Treasury. They announced that private health insurance plans will be required to cover over-the-counter COVID-19 diagnostic tests effective Jan. 15, 2022.

The rule requires insurers to offer the tests to plan members with no member cost share, regardless of medical necessity.

To start, members were reimbursed for purchases from pharmacies using a prescription drug reimbursement or coordination of benefits claim form. But most plans quickly began working on methods to distribute those tests through their preferred pharmacy carriers through a "direct coverage system."

Under the White House program, members of private insurance plans each are allowed eight tests per calendar month. So, for example, a family of four could receive 32 tests each rolling calendar month.

Tests could be individually packed, or they could be bundled — say two or more to a box — and still be eligible for the program.

The program incentivized plans to create a direct-coverage system that eliminates the need for the members to pay up front.

Through direct-coverage plans, members get their tests through their insurer at the point of sale, either through a bricks-and-mortar store by showing their pharmacy benefit card, or through mail order. Members get those tests without up-front costs, provided they use the in-network system.

The benefit to the insurer for setting up a direct system was that plans could then limit how much is spent per test. With a direct system in place, if members use an out-of-network provider, they would still get reimbursed, but with a per-test cap on each test — \$12 per test or less.

Without that direct coverage option, there is no limit to how much each test can be reimbursed for, potentially opening the door to runaway inflation or price gouging.

The program allows insurers to require receipts, and they

may ask members to attest that the tests are for personal use and not for resale, won't be reimbursed somewhere else, and that they aren't solely for employment purposes.

All of this is in addition to the [covidtests.gov](https://www.covidtests.gov) program that rolled out in January that will mail up to two sets of four rapid tests to peoples' homes, paid for by the federal government.

It is important to note that the cost-free over-the-counter program does not directly apply to Medicaid plans, but the Centers for Medicare and Medicaid Services (CMS) does mandate that tests be covered in some way for Medicaid or CHIP policyholders, but the details vary by state.

Medicare Part B and Advantage plans began to offer no-cost tests in April

Some initial reports came in when the tests were first announced saying insurers hadn't been given enough time to update their systems on such short notice to be ready to reimburse members immediately. One challenge was that at-home tests didn't fit neatly into established billing code categories.

Another worry among plans and employers is the cost, and specifically, what those costs will do to premiums in the long run.

With tests averaging \$15 a piece, that would add \$480

in claims for a family of four every month. Over a year, that adds up to an additional \$5,760 in claims if every family ordered the maximum number of tests. Those are claims that were not factored into cost estimates when the annual premiums were set for the year.

With multiple methods of reimbursement, some analysts also worry that unscrupulous members may try to be reimbursed for the maximum number of tests through both the reimbursement system and the point-of-sale options, meaning cross-system record keeping between health plans and pharmacy benefit

plans will become essential.

When the program was initially announced, a run on rapid tests meant that few pharmacies were able to keep them in stock. But at this point supply has largely caught up, and shelves typically have readily available tests.

Still, there is the open question of unplanned costs to insurers, and what that is going to mean for premiums down the road. **CB**

The rule requires insurers to offer the tests to plan members with no member cost share, regardless of medical necessity.



MICHAEL GIUSTI, MBA, is senior writer and analyst for [InsuranceQuotes.com](https://www.insurancequotes.com).

Finance



Leveraging Virtual Assistants for Greater Employee Satisfaction

BY AARON KANE

Amid all the paperwork and reporting, advisors can feel like they have very little time to focus on the most important part of their job: client service. And as your business grows, so do your administrative responsibilities. To provide your clients best-in-class service when grappling with mounds of work, try hiring virtual assistants to do the work the client doesn't see. By prioritizing your client service skills, you and your team can get greater enjoyment out of your work while increasing office productivity.

Designate your priorities

Before hiring any new virtual staff members, you and your team need to take some time to determine which high-priority tasks you need help completing, and what you can continue to manage. Take some time to think about tasks you spend a good chunk of time on that aren't client service-related. For example, if you spend 5 hours a week calling third-party insurance providers, that's 5 hours you could be communicating with clients or meeting with your team. Determine which daily tasks you and your team can pass to the virtual team that will help you all feel more satisfied in your positions.

Virtual onboarding

Once you and your team have identified the tasks you will pass on to the virtual assistant(s), you can begin hiring and onboarding. The hiring process can be fairly simple — find an online outsourcing resource, such as VA Platinum (vaplatinum.com.au), and follow their procedure for hiring virtual assistants, or VAs. Most outsourcing companies have a process to help determine both your needs and what the VA's can best help with. Having an idea of what you want them to help with beforehand will streamline the process and get the VAs on your team sooner.


When onboarding, there will be a lot of detailed information that the VAs need to know before getting started. To streamline the onboarding process, I use an online software: **Monday.com**. Software like Monday.com helps organize tasks and information that the offshore team will need. For example, we use the software to give our VAs access to our process guide library containing all of the information on our clients, the third-party companies we work with, projects similar to what they'll work on, etc. This library allows us to onboard VAs without requiring hours of our time to get them up to speed.

Working together

After the VAs have learned the ins and outs of your busi-

ness, you can set up their daily tasks on a platform like Monday.com as well. Start with simple, non-client facing tasks, such as administration services or organizing email inboxes. This will help them get a feel for your firm and the style of work. Many onboarding programs also allow you to track the progress of an ongoing project, so you have an idea of approximately how long it may take the VAs to complete a specific task. As they become more comfortable with your business and the profession, they will spend less time overall on projects. Then, you can begin to ramp up the type and amount of work they do daily.

The more your virtual assistants can comprehend the intricacies of financial or other services, the greater service they can provide you. For example, my VAs now take prospecting calls, send emails, run credit files and more, because they have a handle on the information that they need to share and record. Though the work that they do may be mostly invisible to clients, it makes a world of a difference for both me and my staff.

The work taken on by our virtual assistants helped my onshore team grow into new roles with greater responsibilities. Due to their increased availability, my onshore team has been able to offer much better client service and they enjoy their jobs now more than ever. Client service is why most of them became financial professionals, so being able to work primarily on those relationships makes their jobs more fulfilling. They are completing tasks that align with their skills, so they are able to spend more time refining their skills and looking for areas of growth in this field. Although clients may be unaware of the amount of administration and compliance work that goes on in the background, advisors often spend countless hours buried in paperwork. This can sometimes lead to clients feeling neglected by their advisor, as the advisor may not always be available. By outsourcing management of more tedious tasks to virtual assistants, you give yourself and your onshore team more time to tend to client needs and improve the efficiency of your practice. 



AARON KANE, FChFP, B Bus, Dip, FS, is a director and shareholder at EK Financial Group in Victoria, Australia. Aaron is a 7-year MDRT member and was a 2013 finalist in the Money Management "Young Achiever of the Year Award."

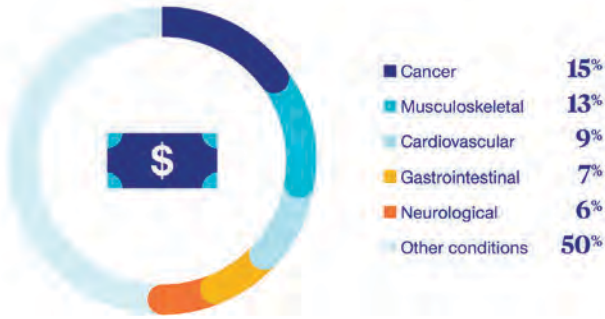


Employer Healthcare Costs Lowered by Increased Transparency

Study reveals top five clinical conditions drive 50% of employers' costs

BY PATTY STARR and CRAIG KURTZWEIL

In an extensive analysis of patient claims data, health plan member engagement has emerged as employers' single best-practice solution for controlling costs and improving outcomes for their employees. In the fifth joint white paper by the Health Action Council and UnitedHealthcare, a comprehensive analysis of 320,000+ covered lives identified 50% of nearly \$2 billion in cost to employers was limited to five conditions.



The study, “Costly Conditions: Identifying and Addressing Top Clinical Cost Drivers” (healthactioncouncil.org/News/Health-Action-Council-and-UnitedHealthcare-Release) offers insights into why employer cost varies so widely across gender, age, income, geography, and social determinants of health. In addressing these dominant conditions, the report shows why individual communities matter so much in terms of total cost of care, billing patterns, treatments, and outcomes. In addition to the “why,” the report shows how employers can reduce costs by encouraging more employee engagement.

Best-practice recommendations

Long-term research by UnitedHealthcare and Health Action Council clearly confirms that policies and practices that shed more light on care and cost choices produced better results for both employers and employees.

Access to better information through innovative resources, industry collaborations and ongoing research advances healthcare equity and reduces costs. Wider access and visibility empowers people to make more informed health and wellness decisions.

For employers, management and budget priorities should focus on these strategic imperatives:

• Transparency:

Empowering people with more information about their care options may help everyone make more informed decisions and save money. Integrated online resources available today provide personalized wellness support, decision-making power, and comparison-shopping options for employees.

Employers can achieve significant gains by providing tools for employees to evaluate providers, treatment options and cost estimates of medical services.

• Engagement:

Encouraging employee engagement/activation helps optimize plans and incentives. For example, the UnitedHealthcare HAI™ tool evaluates 53 evidence-based decisions as well as life-stage, demographic, and social determinants, to identify under-engaged individuals and groups. The report shows that highly activated patients are significantly less costly, and far healthier, than those lower on the activation scale.

• Affordability:

Lower drug prices have the greatest impact on plan affordability for the company and employee. One example is

introducing pharmacy step therapies to support the use of high-quality, lower-cost generics or biosimilars before turning to more expensive solutions. Also, look for differences in practice patterns by geographic region (over- and undertreating; low adoption of best practices) when targeting high-cost conditions. Did you know that neurological treatment differs greatly by location? For example, patients in Greensboro are eight times more likely to have carpal tunnel surgery than people in Phoenix. Billed charges also vary widely.

The average billed by providers in Los Angeles is four times higher than Philadelphia for the same procedure code.

• Advocacy:


Employers should also make sure their employee health strategy includes a commitment to helping their workers navigate the healthcare system. Using advocacy, clinical resources and advanced algorithms to identify the next best action steps personalized to each member, can go beyond basic customer service. These tools help develop a deeper understanding of an individual and their needs, including social needs, to deliver personalized guidance.

The goal is to create a simpler experience, so a person can:

- make more informed health decisions
- improve their health
- connect with relevant clinical programs
- avoid unnecessary costs
- understand lower-cost treatment options
- find community resources

The bottom line for employers

Although healthcare costs can be challenging for any business, the white paper identifies the top five clinical cost drivers. It provides employers with actionable steps on how to address these conditions to help improve employee well-being and lower costs. These steps include providing better price-tag transparency and employee engagement tools. Using analytics and oversight of factors ranging from location of care to drug prices can lead to measurable improvements in health outcomes and cost-of-care affordability.

Employers can learn more about how to lower costs and help employees achieve better health by reading the full white paper here: healthactioncouncil.org/News/Health-Action-Council-and-UnitedHealthcare-Release. 



PATTY STARR is president and CEO, Health Action Council.



CRAIG KURTZWEIL is VP of UnitedHealthcare Center for Advanced Analytics.

Health Action Council is a not-for-profit organization representing large employers to enhance human and economic health through thought leadership, innovative services, and collaboration. UnitedHealthcare is dedicated to helping people nationwide live healthier lives by simplifying the health care experience.



Broker Friendly Carriers Are Valuable Partners

A NOTE OF APPRECIATION FOR ALIGNMENT HEALTH PLAN

BY PHIL CALHOUN

Independent brokers and agents offer their clients more solutions and gain a level of confidence with carrier partners who are proactive with member service, offer competitive plan designs, and commit to a competitively priced and robust provider network. Since books of business values and transfers are more important to more brokers, learning which carriers are truly broker friendly is critical. The service and support of brokers is paramount, but also the commitment and appreciation to our compensation at enrollment, renewal and in retirement helps brokers make long term decisions about carrier partners.

One carrier recently made a strong commitment to both brokers and members: Alignment, a Medicare Advantage Plan. This commitment is worthy of recognition.



CALL OUT

Alignment Health Plan is powered by AVA®, Alignment Healthcare's proprietary technology platform, which stratifies members based on their health status and social needs.

"AVA is a game-changer that sets Alignment Health Plan apart from other Medicare Advantage plans, built to aggregate and analyze member information in a way that empowers our doctors to provide truly personalized care for their patients," said Dr. John Kim, regional chief medical officer, Alignment Health Plan CA. "Through AVA, we are able to predict possible care needs, allowing our care team to proactively engage with our members and intervene when needed to keep our members as healthy as possible."

The move to bring to members the most advanced technology is one of the reasons to shine the light on Alignment. The other reason is this year Alignment has decided to work with brokers who retire from the insurance business and join the majority of carriers with a viable commission transfer process. Carriers with a broker friendly commission

transfer process enable clients and brokers the benefit of a consistent broker relationship after enrollment and also beyond. Without this process brokers have no ability to gain value for their hard work when a carrier has no succession process. In addition, without a broker transfer, clients of a broker who retires or has a life event are left to contact the carrier's 800 number for service and support.

Benefits of commission transfer

While most group and individual carriers have a viable transfer process, in the few cases where a Medicare Advantage and PDP carrier does not offer transfers, members are not serviced at the level experienced by their independent broker. For example, during the Annual Election Period, MAPD and PDP members unattached to a broker will not benefit from the best practice of "shop and compare the market" as carriers are unable to perform this vitally important help. This essentially weakens the ability of the carrier to retain the member. Often the member either moves on and finds an active broker to shop and compare — or stays with what could be benefits and coverage that is less than desired for a member's changing health requirements.

So, thank you to Alignment for the commitment to members and to brokers.

The commission transfer ability is a huge positive nod to the work brokers commit to handle, certify annually and stay current with provider networks and local plan availability. These brokers remain dedicated to the efforts needed to bring the best benefits to their clients for the most competitive price. Brokers who often stay with their top five carriers each year will benefit from taking a deep look at the client and broker commitment Alignment has made and consider adjusting their favorite carrier rankings.


FMOs and GAs

Most brokers work with a trusted Field Marketing Organization (FMO) or General Agency (GA) to assist them to sort through the many carriers and understand plan benefits which change annually. With this support, brokers can

take this knowledge to their clients. The hard work brokers perform to find clients, discover their needs, shop the market, and match them with a benefit package that is in balance with their needs and fairly priced, rounds out how our industry functions in a client driven manner. In addition, when a carrier commits to service and support of both brokers and clients there is a WIN-WIN. Over the years many changes have occurred — new carriers, entities acquiring carriers, carriers merging with other carriers. Through all of this, brokers play a very critical role to bring the plans from carriers to businesses and individuals. Brokers are there to assist clients by sorting through the options and matching them with plans that best suit their needs.

Final thanks to professional associations

Many times it is through the work of our professional associations that brokers can perform the work they do. Brokers are surrounded by the carriers and the plans they offer. So, we want to call out carriers who should be recognized for the efforts made to help brokers serve the public.

Please let me know when you have a carrier you would like to recognize and share your experience. 



PHIL CALHOUN is president of Integrity Advisors. He published "The Health Broker's Guide: How to Protect, Grow and Sell Your Commissions" eBook. Find it free online at

www.healthbrokersguide.com.

Calhoun's goal is to help active brokers reach 100% commission protection and help retiring brokers make the exit planning process work for them. Calhoun consults with brokers statewide. For more information visit www.commission.solutions

phil@commission.solutions
714-612-0306
800-500-9799



How Working Less Might Be Better for Your Financial and Mental Health

DISCOVERING A CLIENT'S MONEY SCRIPT CAN HELP THEM PROSPER

BY CHIA-LI CHIEN

Alice was one of my recent pro bono clients (not her real name, but the facts are real). Alice has been a full-time government worker for three years. She is very stressed about keeping up with her lifestyle, so she works two other part-time jobs. Due to her combined income, her federal tax bracket shifted from 12 to 22%. Alice was shocked that there was no tax refund in 2021 but instead she owed federal and local income taxes.

To explain how this happened, I asked her to describe her situation and what her typical week looks like. Alice purchased a home in Sept. 2021 and believed she would get a deduction from her mortgage interest and property taxes. But she is a frequent sports bar customer and a great tipper.

Additionally, Alice has four golden retrievers and other pets at home. She spends 40 hours a week at her full-time job, 20 hours a week at part-time job, and five hours a week working for Doordash. Voila! – she's created the perfect storm of working more, stressing more and clearing less income.

Cultivate better behavioral finance

There are three financial benefits an individual should consider when making financial decisions, according to Meir Statman's latest book of "Behavioral Finance: The Second Generation." The three financial concepts include utilitarian, expressive, and emotional.

Utilitarian: “What does something do for me and my money?”

Expressive: “What does something say about me to others and myself?”

Emotional: “How does something make me feel?”

In Alice’s case of working three jobs yet spending at the same rate, her utilitarian benefit might justify her working 65 hours a week to make more money. Her ability to frequently visit sports bars leaving great tips gave her the expressive benefit about her financial ability. She felt good about her increased income to afford her lifestyle.

But Alice also demonstrated a hard-wired financial behavior of “money worship & money status” categories in the money script according to Dr. Klontz and Dr. Britt’s book “Financial Therapy: Theory, Research, and Practice.”

A money script is a belief that typically developed in childhood and is hard-wired into adult financial behaviors. There are four categories of money scripts: money avoidance, money status, money vigilance and money worship.

Money Status = financial status equals self-worth. In Alice’s case, she spent as fast as she made money to keep up her money status.

Money Vigilance = individuals stay alert and concerned about their financial health. They tend to save, stay frugal, and be smart about their spending. Alice did not show a money vigilance belief.

Money Worship = individuals believe money is the key to happiness, and the solution is to have more money. In Alice’s case, she works 65 hours a week to have more money.

Money Avoidance = individuals do not deserve money and believe wealthy people are greedy. Alice did not show a money avoidance belief.

After some simple calculations, I was able to illustrate to Alice that working less will help her remain in the lower tax bracket. Alice can afford to work at her full-time job and should forgo her two part-time jobs. She can also afford to visit a sports bar once a month or less to control her spending. Working less for Alice is a solution. I could see the stress coming off her shoulders immediately.

TOOLS TO IMPROVE MONEY SCRIPTS

Several tools can help you learn more beneficial financial and money script beliefs.

1. Statman’s book “*Behavioral Finance: The Second Generation*” is available on Amazon Kindle for free.
2. Visit Dr. Klontz’s website to test your and your client’s money script beliefs: bradklontz.com/moneyscriptstest

To enhance your ability to work with clients and learn more about how to balance financial mental health, consider taking one of the following graduate-level courses.

- The Master of Science in Financial Planning at The American College of Financial Services: Behavioral Finance class: theamericancollege.edu/designations-degrees/msfp
- The MBA in Financial Planning at California Lutheran University: Behavioral Finance class: callutheran.edu/fp
- Creighton University’s online Graduate Certificate in Financial Psychology and Behavioral Finance: creighton.edu/academics/programs/financial-psychology-behavioral-finance

In summary

We all make the financial decisions from three financial benefits and hard-wired money script beliefs in financial behaviors.

An advisor’s ability to recognize the client’s financial benefits and their money script beliefs could help you better lead your clients in the right direction. In Alice’s case, working less was a nice surprise, along with other minor adjustments to control her spending. She certainly did not expect working less to be one of the solutions. In reality, working less will reduce her stress and help her maintain her mental health.

It is critical for the advisor to recognize and help balance the client’s financial and mental health. **After all, not every financial issue can be solved by financial products. ©**



CHIA-LI CHIEN, PH.D., CFP®, PMP®, CPBC, is a succession program director at Value Growth Institute. Before her consulting practice, she held several senior management positions in Fortune 500 companies. Chien is a frequent speaker and has published three award-winning books. She holds a doctorate in financial planning and is a Certified Financial Planner (CFP®).

Chien is an associate provost of graduate programs and associate professor at The American College of Financial Services.

Contact: jolly@valuegrowthinstitute.com.

ARE YOU MEETING THE NEEDS OF YOUR DIVERSE POPULATIONS WHEN IT COMES TO HEALTH BENEFIT STRATEGY?

BY DR. TYLER AMELL

A best practice in any employee health and benefit strategy, particularly those targeted at reducing ever increasing healthcare costs, is to collect Health Risk Assessment (HRA) information and use this data to drive your wellness or wellbeing programming strategy. Once you are able to ascertain the health status of your client's employees, the HRA data act as a baseline to target programming on both a personal and organizational level. Further, they can measure engagement and outcomes across a wide variety of metrics as time goes on, quarter by quarter or year by year. Since most of your health status is linked to the choices you make, and the lifestyle you lead, these are the most beneficial to address from a sustainable behavior change perspective. **It is all about getting people to make better decisions for themselves and their loved ones.**

Examples of programming that is tied to choices and lifestyle include personalized education and training related to your health risk. Topics would include how to get more exercise for your mind and body, eating more balanced meals, drinking more water and less sugary beverages or alcohol, quitting smoking and getting better sleep. In order to be effective, personalization is critical to programming. This personalization is based upon accurate HRA information and associated behavioral data. It is not helpful if someone is a nonsmoker who exhibits good sleep hygiene and patterns ends up with programming targeted at quitting smoking and addressing sleep issues! Same for someone at a healthy weight being provided with weight loss information. It turns plan members off. Programming must speak to individual needs and interests and be tied to risk in order to yield desired outcomes.

Late last year I published an article in the American Journal of Health

Promotion focused on using HRA data to help employers plan for changes in employee health that have occurred during the COVID-19 pandemic. The data revealed that brain health/mental health, including stress, anxiety and depression issues were weighing heavily on employees. Many had health indicators that were deteriorating, or not as positive as they were as we entered the pandemic. Further, preventive health behaviors such as vaccinations and screenings were negatively impacted through a wide variety of influencing factors. This meant that as we moved into future phases of the pandemic, there was some ground to make up from a health perspective. The pandemic reversed some positive momentum that many employees and employers had gained in the period leading up to 2020.

Another notable factor that was exacerbated by the pandemic was the recognition of the relationship between race, sex and gender and health disparities. There are strong relationships between these factors. However, they do not tend to be exhibited in employee health benefit data for a variety of reasons — the most important being lack of reliable data. This is where HRA data can help brokers and employers better address diverse populations in the workforce. This is due to the presence of validated and reliable questions in some National Committee for Quality Assurance (NCQA) certified HRAs. This can help employers stratify data and assure appropriate programming is meeting the needs of diverse populations.

For this reason, I conducted another analysis of MediKeeper's large HRA data set using anonymized data from Jan. 1, 2017 through Dec. 31 2021. This time, rather than limiting the analysis to sex, I included both race and gender. The results indicated that there are substantial differences in wellness platform engagement and health

behaviors when you dig deeper into these data. What is revealed can have a dramatic impact on your wellness or wellbeing programming, and underlying benefit strategy. I presented these findings at the recent Art & Science of Health Promotion conference in San Diego in April 2022.

The data revealed [DTA1] widespread variation in health platform engagement, health risks and lifestyle behaviors by sex and race. Gender was not a significant factor. If these types of data are not analyzed and understood, using appropriate techniques, benefits and programming may miss the mark. In general, over the 5-year period, the racial diversity of those workers using the wellness platform increased. For example, the proportion of African American females increased from 2.1% to 8.5%, an increase of 300%. Similarly, female Asians and Hispanic representation increased 125% and 94% respectively. The proportionate decrease in female Caucasians was 19%. The same trend was seen in males, with increases of African American males of 87%, Asians of 102% and Hispanics of 44%, and a proportionate decrease in Caucasian males of 9%. The very nature of the racial makeup of the population has shifted in the time frame.

When we look at engagement as measured by unique access to the platform by race, all groupings exhibited an increase over the duration of the analysis, from a low 101% in African American males to a high of 630% in African American females. The overall average increase was 342% over 5 years. We can infer that people are increasingly interested in improving their health, or are incentivized to do so, and different races may have different motivations and may require different messaging.

In terms of exercise, female Caucasians decreased their exercise by 1.4%, while female Asians increased

Wellness Platform Engagement by Race

	2017	2018	2019	2020	2021	2017-2021
Male African-American	4.6	6.2	5.9	7.7	9.2	101%
Male Asian	2.0	3.6	4.9	6.0	8.4	312%
Male Caucasian	2.7	3.2	5.0	7.0	8.9	230%
Male Hispanic	1.8	4.2	6.7	7.1	9.3	406%
Male Other	3.6	3.7	4.8	7.0	8.4	132%
Female African-American	2.7	4.9	16.4	16.8	19.8	630%
Female Asian	2.6	3.5	5.7	7.3	11.8	358%
Female Caucasian	2.4	3.5	7.2	11.1	14.2	486%
Female Hispanic	2.2	3.9	7.5	7.6	11.5	422%
Female Other	2.8	4.1	7.2	4.2	12.5	343%

Received Professional Help for Anxiety or Depression by Race

	2017	2018	2019	2020	2021
Male African-American	7.90%	5.40%	5.80%	5.10%	7.50%
Male Asian	4.20%	5.00%	8.10%	3.30%	6.40%
Male Caucasian	6.90%	6.90%	7.20%	7.30%	12.50%
Male Hispanic	4.40%	3.40%	6.90%	5.40%	10.00%
Female African-American	11.10%	12.00%	11.10%	9.20%	14.60%
Female Asian	6.20%	8.50%	10.80%	5.50%	7.50%
Female Caucasian	14.70%	14.60%	15.60%	15.50%	28.80%
Female Hispanic	9.50%	9.40%	12.40%	12.20%	20.20%

by 23.4%. African American females increased by 16.5% and Asian males increased by 15.8%. For those interested in exercising more, both male and female African Americans and Asians indicated a willingness to increase, while male and female Caucasian and Hispanics were interested in decreasing their level of exercise commitment.

Brain health/mental health is a key area for many employers and benefit plan sponsors, and so data by sex and race is a very useful way of assessing programing needs. Male and female Hispanics increasingly sought professional help for anxiety or depression during the study period, with a 129% and 114% increase respectively. All other races increased as well, indicating a need for these types of services, with the exception of African American males, which exhibited a decrease of 4% over the period. Perhaps outreach programming targeting these individuals will help this

segment of the working population.

Similarly, stress levels increased in all races except male Asians (-10%) and female African Americans (-2%). Large increases in stress levels were seen in male African Americans and female Hispanics, a seemingly different demographic. It is apparent that different races have seen their stress levels vary during the past five years,

which could be a reflection of the nature of their organizational roles.

Based on this analysis, we can safely say that if you have a racially diverse workforce, and are using a one-size fits all approach to your health strategy, it may not be reflective of the wants and needs of the population the benefit plan is designed to support. CB



DR. TYLER AMELL is an internationally recognized thought leader on the topic of workplace health and productivity and Chief Health & Strategy Officer at MediKeeper. He also serves on the executive board of directors of the National Wellness Institute and the Work Wellness Institute. In the past, he served on the executive board of directors of the Integrated Benefits Institute (IBI) and the Canadian Association for Research on Work and Health. He was a past partner and vice president at a global HR consulting and technology company, CEO of a HR technology company and vice president of Canada's largest independent health care, occupational rehabilitation, and return-to-work company. Dr. Amell holds an adjunct faculty position at Pacific Coast University for Workplace Health Sciences. He has given seminars and presentations at more than 250 events globally.

Contact: tamell@medikeeper.com, Medikeeper.com

Taking PRIDE: How Benefits Support Inclusivity

BY ANN COSIMANO

June's Pride Month is a great time to celebrate our diversity and the accomplishments of the LGBTQ+ community and its advocates — but also to take stock in how well we're doing in creating a more equitable workplace. Inclusive benefits play a major role in that effort. And as brokers, your work with employers can help provide the community with the support they need.

Of the 11 million people who identify as LGBTQ+ in the U.S., 88% are currently employed. ([lgbtmap.org/file/LGBT-Workers-3-Pager-FINAL.pdf](#)). Now, in its 20th year, the Human Rights Campaign's 2022 Corporate Equality Index (CEI) ([reports.hrc.org/corporate-equality-index-2022](#)) shows how corporations across the U.S. are adopting equitable workplace policies, practices and benefits for this 8+ million-strong community within the labor force. In its most current report, CEI noted that 44 new pro-equality laws were passed in the 2021 legislative season. They highlight the considerable progress made by the 800+ companies they've evaluated in their commitment to tangible, LGBTQ+ focused diversity, equity and inclusion programs.

While great progress has been made in supporting LGBTQ+ employees in recent years, there's still room for improvement. On the benefits side, brokers and employers should look for potential gaps in areas like access to equitable healthcare, family-starting benefits and financial well-being.

In addition, there can be legal issues associated with many of those areas. This makes a voluntary benefit like legal insurance or legal plans — that provide employees cost effective access to legal counsel, education, and aligned resources — an attractive complementary offering.

Consider some of the issues that members of the LGBTQ+ community may need to navigate over time.

Accessing health care

According to CEI, 86% of participating businesses now offer transgender-inclusive health insurance coverage. But keep in mind — many members of the LGBTQ+ community are still afraid to seek medical care; sadly, 35% do not engage with the health care system at all. The Healthcare Equality Index ([reports.hrc.org/healthcare-equality-index-2020](#)) reports that it's largely because they don't feel comfortable speaking candidly with their health care providers. Seventy-three percent of transgender respondents and 29% of lesbian, gay and bisexual respondents said they feel like they would be treated differently by medical personnel due to their LGBTQ+

status.

For those reasons, Walmart introduced the Included Health platform ([includedhealth.com/](#)), designed to provide comprehensive care tailored to LGBTQ+ employees. With this digital platform, associates can take advantage of concierge services that specialize in connecting LGBTQ+ people and their loved ones with quality, affirming care.

Financing the future

This community can face some distinct financial challenges:

- LGBTQ+ borrowers feel weighed down by student loan debt, especially those with little or no support from family or outside financial advisors. That debt burden keeps the vast majority (87%) from reaching other key milestones, like owning a home, starting a family or saving for retirement.
- Same-sex borrowers are 73% more likely to be denied a mortgage, despite being deemed "less risky" as borrowers. And according to a 2019 study completed by Iowa State University, 26 different states do not have statewide housing protections for the LGBTQ+ community, making recourse challenging.
- A 2021 U.S. Census Household Pulse survey shows more LGBT adults living in households with economic insecurity (37%) than non-LGBT adults (26%).

As we've seen in healthcare, digital institutions are being created to fill the void and serve the needs of the LGBTQ+ community — this time in banking and finance.

Like many of their colleagues, LGBTQ+ employees welcome benefits that help them get back on the road to financial well-being — such as financial education, student loan repayment help, or emergency savings accounts. But should financial issues become legal issues, employees and their partners can tap into their legal plan to navigate a range of challenges from loan refinancing or consolidation to consumer protection matters or personal bankruptcy.

Starting a family

Increasingly important to companies' DEI initiatives are a range of benefits offered to help build a family — regardless of an employee's gender, sexual orientation, medical condition, whether single or partnered. These offerings might cover fertility treatments like IUI or IVF, elective egg freezing, surrogacy, adoption support and reimbursement allowances. Everyone's family planning journey is different. And more companies recognize this and are stepping up with benefits to

support those journeys.

That's great progress — but challenges remain. Establishing parental rights, whether through adoption or surrogacy, can be complicated. Marital status can make a difference in what benefits, rights and privileges LGBTQ+ employees can receive. In certain states, the law won't recognize a queer couple as coparents unless official adoption documentation (known as second-parent adoption) is signed.

One of my peers, Matt Duke, Esq., who works for the Offices of Fears Law in Dallas, Texas, spoke to these real-life challenges during our conversation.

"Whenever I talk to an LGBTQ+ client, it tends to be about family," says Duke. "I had a client whose partner had given birth through in vitro. [My client] wasn't on the birth certificate, and the birth mother didn't want to put her on — and then they broke up. My client was having a really hard time trying to get some sort of custody. Custody is a major thing. When a non-birth parent is seeking custody, that can be really tricky."

All of these proceedings and required processes can create added stress that weighs on your clients' employees. Having an attorney can simplify matters by providing guidance and drafting the agreements needed to protect the employee's interests, family and future. Legal insurance providers, including ARAG, offer members diverse coverages so they can complete critical documentation, from prenuptial or domestic partnership agreements to parentage orders, surrogacy agreements, adoption contracts and more.

Creating a supportive corporate culture


A good place to start could be to review company content for engendered language. Look especially closely at language used in company and benefits policies, job descriptions, and your intranet and HR systems for how well it reflects your firm's work environment. Updated language can communicate volumes to current and prospective employees.

Inclusive language can also help nonbinary/trans employees feel more at ease and valued. Adding their pronouns to an email signature can be an opportunity to be true to themselves at work. But going through the system to legally change their assigned gender on important documents, such as a driver's license, can be daunting. Since how states handle this change varies, it's prudent to consult an attorney for the most up-to-date information and steps they can take to address their particular situation.

My company's values include an essential titled "Be You." To me, this is the most important of the essentials we have identified as critical to the success of our business. An employee who feels accepted, supported and understood will be more likely to bring all their gifts to our workplace.

When an employee is able to show up as themselves, I believe they provide better service, are more productive, less stressed and we have lower employee turnover. This is why I think the work of our employee-run LGBTQ+ subcommittee is so important. It provides an avenue and a resource for our LGBTQ+ employees to not only feel involved but also provides a mechanism for the entire organization to learn what it means to be an ally and how to be there for each other.

Good for all

A benefits infrastructure that is inclusive of LGBTQ+ workers and their families can lead to proven increases in recruitment and retention of talented and diverse workforces. As companies continue to level the playing field for LGBTQ+ workers — it'll not only benefit the community, but it'll also be good for business. 



ANN COSIMANO is ARAG's General Counsel and directs the company's legal, regulatory, compliance, risk management and attorney relations departments. Having started her career as an attorney for nonprofit organizations, Cosimano brings a full understanding of — and deep respect for — members experiencing legal issues. She genuinely cares about improving the lives of others and aligns those values with her role as an executive leader.

<https://www.araglegal.com>



Positioning My Agency

FOR SALE

Success is in the details

BY AMY EVANS



In October 2021, my employee benefits agency was acquired by Shorepoint Insurance Services, an Acrisure agency partner, and I joined Shorepoint as an associate vice president of Employee Benefits. California Broker Magazine asked me to write about my experience in a four-part series. In the first installment, I shared my reasons for wanting to sell my agency, and the challenges I encountered while building my exit strategy. In this installment, I'll share the steps I took to position my agency for sale.

There are many steps I am glad I took that helped me to position my agency for sale. Let me say up front that you can absolutely establish, grow and sell an agency without taking these steps — this isn't a "must do" list. However, having gone through the sale process, I can say that taking these steps allowed me to negotiate the maximum value for my agency and they made the due diligence process as easy as possible for both me and my buyer.

I treated my business like a business.

My agency was incorporated, licensed and insured as a stand-alone corporate entity. There was some additional expense to establish and maintain the corporation, but keeping it as a separate entity allowed me to set up separate banking, accounting and taxes. This made it easy to provide information during the due diligence process and it simplified the transition after the sale.

I kept my accounting up-to-date.

I worked with a CPA, tracked and categorized all of my expenses and ensured that I was meeting all of my tax obligations. I was able to produce a clean Profit & Loss statement for my agency, which helped the buyer understand the overhead they would be assuming, and helped me understand the overhead I would be giving up after the sale. Because I used good accounting software, my CPA and I were able to run reports as the buyer requested them, making the due diligence process as efficient as possible.

I used an agency management system to track policies, commissions and carrier contracts. While entering data often felt tedious (and I eventually outsourced this work), having all of my policy, commission and contract information readily available gave me a clear picture of the value of my agency. I was able to easily communicate valuable information to my buyer: number of groups and policies in force; revenue by group, by carrier, by line of business; revenue in the small group market vs. the large group market. During the due diligence process, I was able to provide information down to policy number, renewal date and commission rate per policy. After the sale, having this information readily available simplified the transfer of my groups to my new agency.

I had a clear understanding of my agency's value and growth potential. Tracking policy and commission information meant I could project revenue for the next 12 months. I could see which groups were profitable due to organic growth. I could also identify opportunities to sell additional lines of

business. With my agency, I knew that my previous 12 months of revenue were not as compelling as my next 12 months of revenue, based on recent account acquisitions and projected organic growth. I was able to tell a compelling story to my potential buyers about the future value of my book of business, supported by my strong network of referral partners and my marketing efforts, including my AlignWomen Podcast. (alignwomenpodcast.com)

Taking these steps gave me the ability to speak intelligently about my agency when I started having conversations with potential buyers. It also gave me confidence that what I was selling had real value. And it gave my potential buyers confidence that they were making a solid investment.

In my next installment, I'll share how I found the right buyer for my agency. 📌



AMY EVANS is now associate VP at Shorepoint Insurance Services.

She has more than 20 years of experience in the insurance industry, simplifying employee benefits for employers and their employees. In October 2021, her insurance agency was acquired by Shorepoint Insurance Services, an Acrisure Agency partner, and is now operating under the Shorepoint name. As an associate VP with Shorepoint, Amy works with employers to help them navigate the complex world of employee benefits, business insurance and risk management.

Amy is passionate about empowering professional women to network more effectively. In 2019, she founded AlignWomen, a leadership and networking organization for professional women. She is also the host of The AlignWomen Podcast, which features female entrepreneurs, leaders and other professionals who have demonstrated agency and innovation in their personal and professional lives. (alignwomenpodcast.com)

Amy is a frequent speaker, writer, podcast guest and social media participant and you can find her engaging regularly on a variety of topics including health insurance issues, entrepreneurship, social media strategies, women's empowerment and networking with intention.

Contact: **323-633-2263** | amy@shorepointinsurance.com
www.shorepointinsurance.com



CAN STATE LONG-TERM CARE PLANS ALONE SOLVE THE LONG-TERM CARE PROBLEM?

BY CHRISTINE MCCULLUGH

The Long-Term Care (LTC) community knew this was coming — a time where the impact on state Medicaid programs due to the aging population, and lack of knowledge of the responsibility for personal LTC planning, would drive actions for employers and individuals to purchase long-term care insurance. Why? To sustain Medicaid.

Let's explore what happened in Washington State, what is being contemplated in California and what employers are doing to assist their employees.

In 2019, Washington State legislature passed an employee LTC payroll tax — the first of its kind law to help fund the state dollars paid out to nursing homes and alike for long-term care. The tax itself is not a penalty, rather it is an upfront payment towards a state LTC fund. The goal is to reduce overall

Medicaid spending on LTC services through private insurance or public and private combined.

The WA Trust Act established a state LTC plan (wacaresfund.wa.gov) funded by employees in Washington from their paycheck at 0.58% of total wages, uncapped. Although the tax collection has been delayed until 7/1/23, the requirement to purchase a LTC plan prior to 11/1/21 to file for a tax exemption did not change.

Additional highlights of the WA Care Fund & requirements:

- A one-time opportunity to opt out of the payroll tax by completing two steps:
 1. Proof of a private LTC plan purchased prior to 11/1/21.
 2. Submission of Request for Tax Exemption Application to the state website (wacaresexemptions@esd.wa.gov) to be approved or declined by the state.
- The application for tax exemption must be submitted between October 1, 2021 and December 31, 2022.
 - Purchasing coverage after 11/1/21 does not meet the tax exemption requirement and the resident would be responsible for the payroll tax.
 - A proposed re-attestation every year or three years to prove the qualifying coverage remains active.
 - The WA Cares Fund pays for care provided in Washington State only.
 - The policy lifetime benefit is \$36,500.
 - Inflation protection is built into the long-term care plan.
 - Qualifying for the benefit requires a vesting period based on how long the employee has paid into the plan. Full benefits require 10 years of payments (tax) into the program without an interruption of five or more consecutive years. In addition, for individuals born before Jan. 1, 1968 with a contribution for at least one year, a partial benefit for lifetime coverage is

available.

Washington State's bold step started a national conversation among states. California has a task force exploring a government-funded long-term care plan. The timeline for the CA Task Force is to deliver a feasibility report by 1/1/23 and an actuarial report on recommendations by 1/1/24. Once the two reports are approved, state lawmakers will work through the legal process to adopt or deny the recommendations.

As the CA Task Force is designing a LTC plan, they are taking into consideration challenges with the WA Trust Act to avoid problems and deliver a truly valuable program for all constituents within the state.

As the CA Task Force works through their process, many other states are watching and considering an effort like Washington State. To name a few — Alaska, Colorado, Hawaii, Oregon, Illinois, Michigan, Minnesota, New York and Utah — are carefully watching WA and CA.

In this new era of financial planning and advice, consideration by employers to help employees get ahead of this trend is important for several reasons:

Providing education on long-term care.

What is LTC, the cost and risk of needing care. What are the devastating effects a LTC event can have on an employee's savings, investments, home, and family?

Communicating key options and benefits of private long-term care.

Employers' LTC plan can provide employees a comparison to a state-sponsored plan. This allows employees to decide which plan is best suited for their needs.

Explore LTC insurance now. Have enough time for thoughtful research of LTC products and appropriate timing to successfully implement a LTC plan, in advance of a state plan. This will remove the concern of the carrier's ability to provide quotes and enrollment dates.

Employers offering a plan and employees already enrolled in long-term care plans are commended for their efforts and actions to help reduce Medicaid payouts and for protecting individuals' assets. Moving forward

solving the overwhelming long-term care funding issue will take a collaborative effort between the state and private sector. Establishing an acceptable tax rate and designing a plan providing value for residents will be impactful. Providing the tools and education for private long-term care policies is equally important for residents with significant assets and potential care needs. The challenge remains to encourage and motivate employers and employees waiting on the sidelines to take action. **CB**



CHRISTINE MCCULLUGH

is the founder and president of LTC Solutions, Inc. established in 1996. LTC Solutions, Inc. celebrates 26 years in the industry and

holds a certification of Women Owned and WBENC (Women's Business Enterprise). Christine is recognized by insurance companies, benefit brokers and employers as a national expert in LTC insurance. She is a speaker and consultant helping shape the future of LTC insurance. She provides expertise with the utmost relative and current data regarding the LTC market. She has been actively involved with the WA State Trust Act and in March 2021 she testified at the WA Senate Health and Long-Term Care Committee HB 1323 supporting an amendment to extend the opt out to 12/31/21. In 2021, Christine provided WA Trust Act educational webinars to hundreds of employers and brokers in Washington State. She closely follows the CA Task Force as they work on designing a plan for California. Christine is also a member of the National Association of Insurance and Financial Advisors (NAIFA)-LTC Study Group.

**Contact: cmccullugh@ltsolutions.com
1-425-284-2742**

LIFE SETTLEMENTS

How You and Your Client Benefit from Both Sides of the Life Insurance Settlement Coin

BY LISA REHBURG with BRIAN J. CLARK

LISA REHBURG

By now, you have heard me say that 500,000 seniors a year will lapse their life insurance policies, walking away with little or nothing. You may also already know that life insurance policies can be sold through a life insurance settlement. But, did you know there are actually two ways that you can help your clients and potential clients with life insurance settlements? Let's talk about them both.

The first side of the life insurance settlement coin is what is briefly outlined above. Your clients may have unwanted, unneeded or unaffordable life insurance policies and may not know what to do with them. So many times, the only option they think they have is to lapse or surrender the policy. Not true!

You can help your clients by introducing them to the concept of a life insurance settlement. A life insurance settlement is simply a financial transaction. A buyer pays a client a lump sum of cash. In turn, the buyer will become the new owner of the policy, pay the premiums and become the beneficiary.

A client may wish to consider selling their policy when the policy no longer serves the purpose for which it was purchased. Perhaps the house is now paid off, a spouse has passed away, the kids are gone, a business has been sold. Or, perhaps the policy has just gotten too expensive to maintain, or the premiums do not fit into a retirement budget. Or, sometimes, clients may just want to repurpose a policy to make their life more comfortable, like being able to afford assisted living, home care, memory care, or help them age in place. Whatever the reason, and there are obviously 500,000 different reasons, a life insurance settlement can make sense.

The good news is that you do not need to be the writing agent on a client's life insurance policy, or even write life insurance. These clients could be your Medicare, small group, long-term care or individual clients, for example. And, perhaps it is not your client, but your client's parents or grandparents that have policies, or even one of your family members. We have helped some insurance agents sell their

own policies. The bottom line is the opportunity is endless, especially since the population of seniors in the United States is set to grow to 70 million by 2030.

Remember, all different types of policies can be sold, including term policies. On average, selling a policy generates 3 to 5 times cash surrender value. And, the life insurance settlement market has been legal since 1911 and is highly regulated by Departments of Insurance across the country. Think about your client's life insurance policy as an asset that they own (because it is), like their car or their house. Would you want your client to give away their house, and walk away from it? Of course not.

The best news is — your clients will thank you. It is a “win” for them because they are getting more money for this asset than they would have if they have lapsed it or surrendered it. It is a “win” for you in the form of commission from the sale, but also an opportunity for additional product sales once your client receives the money. Annuities anyone? Long-term care insurance? You get the idea.

But, that is only one side of the life insurance settlements coin. To make the life insurance settlements market work, there have to be buyers. When there is a supply of policies (i.e. 500,000 seniors a year), there has to be a demand for someone to buy them. Who are these buyers? Why would they want to buy a life insurance policy? And what does this mean for you and your clients? I am turning the conversation about the second side of the life insurance settlement coin over to Brian Clark, an expert on the investment side. Take it away, Brian.

BRIAN J. CLARK:

Thank you, Lisa! Now that you know all about how you may be able to help people extract significant value from an unwanted, unneeded or unaffordable life insurance policy, let's look at how you can help other clients add some true diversification to their investment portfolios. I focus on helping agents assist their clients where appropriate to invest in this most unique asset class known as life insurance settlements.

The reasons why this type of investment can make sense in one's portfolio are many and the benefits potentially quite significant. And, while there are risks to be aware of, if done properly, owning life insurance settlements as an investment can improve one's investment portfolio. Historically, life settlements have been used primarily only by large investors, such as Warren Buffett, Blackstone and other institutional investors like hedge funds, national pension funds and endowments. Here in California, however, there is unique legislation that allows you to offer this investment to financially qualified California individual investors using only your life license!


Back in the year 2000, legislators in Sacramento passed CA Senate Bill 1837, which established an exemption in the state securities law and regulates life insurance settlement investments. The subsequent law allows agents with a valid CA life license to offer this investment to California individual investors who have a minimum net worth of \$250,000 excluding the value of their home, cars and home furnishings. That means a large percentage of your clients could potentially qualify. You are in an excellent position to add significant revenues to your practice as you help these clients invest in life insurance settlements in their investment portfolios to add true diversification that doesn't sacrifice performance potential. If appropriate for the client, they may even elect to use IRA or Roth IRA funds to make the investment.

When you think about it, many clients have their investment portfolios invested in what I like to call, "the usual suspects" — i.e. stocks, bonds, real estate, cash, annuities, life insurance and maybe a few other things like precious metals, commodities, currencies or even crypto these days. But at certain times, the performance of most of those things can influence each other, possibly in a negative way at a time that is less than ideal, like shortly before or after retirement. An investment in life insurance settlements is uncorrelated to any other investment they may hold, leading to an increase in the level of diversification in their portfolios. In addition to this lack of correlation, there are a few other key reasons why the big, smart players like Mr. Buffett have utilized life settlement investments in their portfolios.

The payouts from life settlement investments come from some of the largest, oldest and strongest companies in the world: namely, U.S. highly rated life insurance companies. You probably wouldn't be in the business that you are if you weren't confident in the claims-paying abilities of these entities. Also, the payouts are known and are not a matter of if, but when. Not many asset classes can make these claims. Finally, what about the performance of life insurance settlements as an investment? In 2013, the London Business School published a decade-long empirical study examining the expected performance of a very large portfolio of life settlements. The portfolio held over 9,000 policies worth more than \$24 billion. The study concluded an expected average annual performance of 12.5% per

year. The conclusion of the study was that the asset class of life settlements can deliver stock-market-like performance without the volatility or risk that is inherent with stock investing.

An individual's actual performance from a life settlement investment may vary significantly. There are risks, such as longevity and liquidity risks among others. However, all of the above reasons should encourage you to take a deeper look into this unique and lucrative opportunity to assist clients with their retirement planning. Find a trusted partner with knowledge and experience; do your due diligence and get started today, because the environment we find ourselves in may result in the next 12 years in the primary markets not being as smooth as the last 12. An investment that is insulated from market turmoil may prove quite valuable to your clients' portfolios.

You now have a better understanding of both sides of the life settlement coin: how you can help clients sell an unwanted, unneeded or unaffordable life insurance policy AND how to help other clients potentially profit from life settlement investments, either with a cash investment or an IRA or Roth IRA investment. You will be fairly compensated for assisting clients with either or both sides of this unique offshoot of the life insurance business! 



BRIAN J. CLARK is the CEO of Alternative Strategies Resource Partners. Brian has more than 20 years of experience helping agents and advisors with solutions that assist their clients in getting to and through retirement in a more comfortable and efficient manner.

Contact: **1-760-668-5440, brian@asrp12.com or www.asrp12.com.**



LISA REHBURT is president of Rehburt Life Settlements, a life insurance settlements broker. Rehburt is energized by helping brokers and their clients benefit from unwanted or unneeded life insurance policies. By having access to many investor groups, Rehburt Life Insurance Settlements can place more policies and realize a better return for clients. Rehburt has been working with brokers in the

health and life insurance industries for over 30 years.
Contact: **1-714-349-7981, lrehburt@aol.com or www.rehburtlifesettlements.com**

ad index

2

Brand New Day
bndhmo.com/brokers
866-255-4795

3

CaliforniaChoice
calchoice.com
800-542-4218

5

Alignment
partnereperience@ahcusa.com
888-793-5700

7

Covered California
coveredca.com/forsmallbusiness
844-332-8384

9

Petersen International Underwriters
piu.or piu@piu.org
800-345-8816

10

Integrity Advisors
Broker Consulting Division
Phil Calhoun MBA
phil@commission.solutions
800-500-9799

11

BenefitMall
benefitmall.com
800-350-0500

47

United Healthcare Services
uhc.com/casave

48

Word & Brown
WordandBrown.com
(Northern CA) 800-255-9673
(Los Angeles) 800-560-5614
(Inland Empire) 877-225-0988
(Orange) 800-869-6989
(San Diego) 800-397-3381

classifieds

**PAYING TOP DOLLAR
FOR
BOOKS OF BUSINESS**

**We Don't Just
Buy Them
We Service Them**



Contact George At:
George@Geldin.com
877-789-5831

Classified Ads



Please contact
Thora Madden
818-370-1706
Thora@calbrokerMag.com

"TOP \$\$ PAID"

**ARE YOU
SELLING?**

MEDICARE BOOK

Call Kevin:
Save-on Insurance
1(888)-613-2626

37 Years Experience

EMAIL:
KEVIN@SAVE-ONINSURANCE.COM

E&O

**LOWEST RATES
IN THE
INDUSTRY
GUARANTEED!**

ErrorsAndOmissionsOnline.com

800 399-3125

OPPORTUNITIES

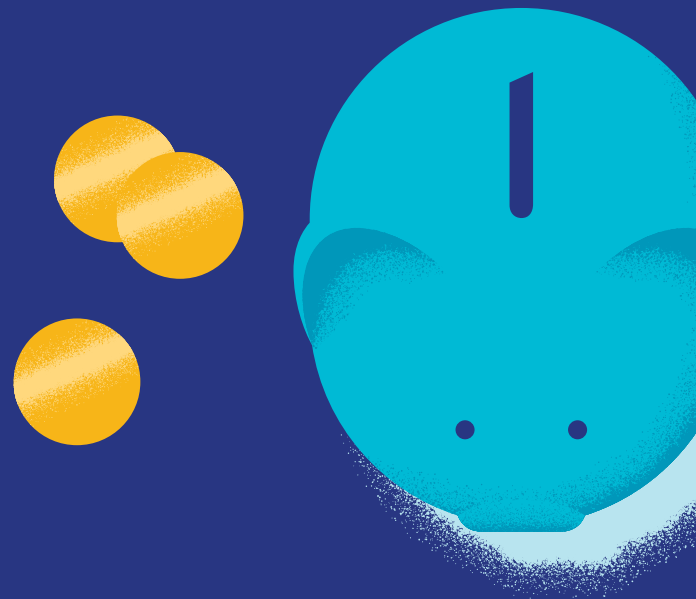
**If you'd like to discuss advertising opportunities,
email Devon Nuszer devon@nustepinsurance.com.**



\$13,390* health plan refund for your business?

Now, that's refreshing.

A health plan refund is possible with **UnitedHealthcare Level Funded health plans**—now available in California. Level Funded is based only on your plan participants. So if their medical claims are lower than expected, your health plan may get a surplus refund at year-end. New UnitedHealthcare Level Funded health plans: all part of our commitment to health care for your life.



Contact your UnitedHealthcare representative for details or visit uhc.com/casave



More savings

Exemption from many Affordable Care Act regulations and state premium taxes



More flexibility

A variety of plan designs, including wellness programs and telemedicine at no additional cost to plan participants



More stability

Fixed monthly plan costs and safeguards to help protect your plan from unexpected high claims

*Yep, that's a real number. Among the 67% of UnitedHealthcare's Level Funded California business customers who received a refund in 2021, the average refund was \$13,390. UnitedHealthcare internal reconciliation analysis, Jan. 1, 2021 through Dec. 31, 2021. Please consult a tax and/or legal advisor to determine if, by receiving this refund, there are any restrictions or obligations. Surplus refund available only where allowed by state law.

Administrative services provided by United HealthCare Services, Inc. or their affiliates, and UnitedHealthcare Service LLC in NY. Stop-loss insurance is underwritten by All Savers Insurance Company (except CA, MA, MN, NJ and NY), UnitedHealthcare Insurance Company in MA and MN, UnitedHealthcare Life Insurance Company in NJ, UnitedHealthcare Insurance Company of New York in NY, and All Savers Life Insurance Company of California in CA.

United Healthcare



REDEFINE PARTNERSHIP.

We make it possible.

Have you thought about reevaluating how you work? Balancing business with more of what you love. We make it possible. We're changing what you can expect from your General Agency.

More than just a quote, we're a team that understands the value of collaboration, in business and in life. An ally that has your back and cares about your success.

Together, let us redefine partnership.

wordandbrown.com

Word&Brown[®]