

Proactive Steps Can Mitigate Risks and Consequences of Data Breaches

The cost of healthcare data breaches keeps increasing, as reported by *Chief Healthcare Executive* (July 24, 2023). According to IBM Security, an artificial intelligence-driven cybersecurity company, the average healthcare data breach now costs \$10.93 million, an 8% increase from 2022. Since the COVID-19 pandemic, the average healthcare breach cost has increased by 53%.

Limor Kessem, Senior Cybersecurity Consultant at IBM Security, attributes the rise to the healthcare industry being a prime target for attackers. One prime example was the HCA Healthcare attack in July 2023, when 11 million patients' information was released by an unauthorized party, making it one of the largest data breaches in 2023 and underscoring the vulnerability of breaches in this sector.

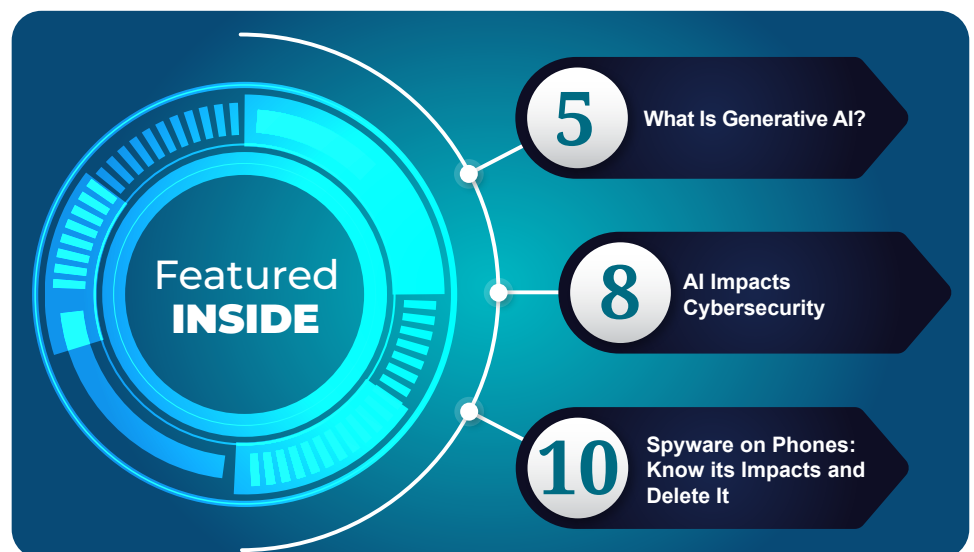
Another example was a cyberattack on Change Healthcare (CHC), an independent healthcare technology company owned by UnitedHealth Group (UHG), which took place in February 2024. BlackCat, a ransomware



group, claimed responsibility for the attack, and according to the CHC HIPAA (Health Insurance Portability and Accountability Act) Substitute Notice webpage (updated August 8, 2024), law enforcement and security experts' investigations confirmed that there was a significant amount of stolen data between February 17 and 20, 2024. Although CHC does not have exact confirmation

on what data was impacted, they surmised that individuals' contact information, health insurance information, medical history, billing and payment information, and other personal information were affected. CHC announced the stolen data in April 2024 and began notifying affected customers in June,

Continued on page 4



From the Desk of Steve Hirsch

Hi Everyone,

As this is my first issue of *Bits & Bytes*, I thought I would first introduce myself, and then write about a popular topic nowadays - artificial intelligence (and I assure you that I am not using AI to write this). I come from many years working on the clinical side of behavioral health, having worked as a psychiatric screener for more than 25 years, the program evaluator for a Certified Clinical Behavioral Health Clinic (CCBHC) expansion grant, and most recently, as the Director of Social Services at Trenton Psychiatric Hospital. In addition, I was the grant manager for the State Targeted Opioid Response Initiative (STORI) for the Division of Mental Health and Addiction Services (now called the State Opioid Response, or SOR). My undergraduate degree was in psychology, and I have an MBA and an MSW (with the corresponding LSW license).

At this point, you are probably asking, "So, how does this all that background fit in with technology and the IT Project?" Well, other than knowing how far behind the times behavioral health care is in terms of the level of sophistication of technology used, I also left the behavioral health field back in the late 90s for a few years and supported the network and the users for News Digital Media (NDM), the company that developed all the web content for Fox Television, Fox Sports, and Fox News. While with NDM, I assisted in the planning and building of a new office, including creating the network infrastructure from the ground up and supporting more than 100 people. For all you Jack Bauer and "24" fans out there, the office we built was used in the filming of the first three episodes of the series.

Since returning to behavioral health, I have been searching for a way in which to merge the two fields in order to better serve the vulnerable populations of New Jersey. Too often, I have seen staff overwhelmed by the need to document the same thing in numerous places (and don't even get me

Continued on page 3

"Bits & Bytes, the IT Project's newsletter, is an excellent resource which provides useful, relevant and up to the minute information. It's an exceptional newsletter, and just what CEOs and executive team members need to stay on top of cybersecurity and trends in the behavioral health field."

Regina Widdows, MA

President & CEO, SERV Behavioral Health System, Inc. and NJAMHAA Board Member



(Continued from page 2)

started on the Unified Services Transaction Form and Midas). Or having to search through documents you thought you completed, but are being told that there are items missing. Or needing to leave a document in order to find information you can only find in another area of the chart. These are just a few of the items that I know made work more difficult for me, as I found myself treating the charts instead of the consumers. Now, as NJAMHAA's Vice President of IT, Human Resources, and Administrative Services, I can look for solutions that address these headache-inducing occurrences.

This is a nice segue into AI as it can assist with decreasing the workload on staff, and allows them to spend more time with the consumers. In the short time I have been with NJAMHAA, I have researched several AI solutions that seem to address the concerns I mention above. But, AI really is only meant to be an assistive device, rather than a replacement for people (and let's not bring up Skynet here - we'll save that discussion for another time). While it is nice to have a laundry list of ideas to choose from, we still need to be able to communicate our clinical judgment to others through documenting accurately and descriptively. One of the criticisms of AI in behavioral health care has been that it comes up with outlandish notes that have nothing to do with what was discussed in sessions. This may be a little exaggerated, but it still is imperative that once the AI notes are created, that the clinicians review them for accuracy. Even though having to review the AI created documents may decrease the overall time saved, it will still save time by preventing clinicians from formulating erroneous treatment plans, and thereby helping to maintain and even increase quality of care and positive outcomes.

That's all for now. More on AI in the future!!!

Steve Hirsch

Steve Hirsch, LSW, MSW, MBA

Vice President, IT, HR and Administrative Services

IT Project Help Desk

✉ ITHelpDesk@NJAMHAA.org ☎ 609-838-6064

STAFF CONTRIBUTORS

Board Chair Anthony Comerford, PhD

Editor & Publisher Debra L. Wentz, PhD

Editor in Chief Steve Hirsch

Editor Shauna Moses

Writers Steve Hirsch

..... Ron Gordon

..... Farrah Fabrigas

Graphic Designer Farrah Fabrigas

New Jersey Association of Mental Health and Addiction Agencies, Inc.

3635 Quakerbridge Road, Suite 35

Mercerville, NJ 08619

Tel: 609-838-5488

Fax: 609-838-5489

njamhaa@njamhaa.org

www.njamhaa.org



Copyright © 2024 New Jersey
Association of Mental Health and
Addiction Agencies, Inc.

Reproduction in any manner,
except as authorized by the
Copyright Act of 1976, is
prohibited.

All rights reserved.



Proactive Steps Can Mitigate Risks and Consequences of Data Breaches

(Continued from page 1)

providing general notice to inform their patients and members. As reported by *The Minnesota Star Tribune* (July 16, 2024), UHG anticipates the cyberattack to cost them \$2.45 billion for 2024, which includes the company's direct response to the breach and losses due to business disruption.

Healthcare cybersecurity defenses lag behind other industries, partly due to difficulty attracting top talent, who often prefer high-paying sectors. The financial industry follows with an average breach cost of \$5.9 million, while the pharmaceutical industry ranks third at \$4.8 million.

The vast and diverse data that healthcare organizations manage, as well as numerous vendor partnerships, make them particularly susceptible to attacks. "It's a big attack surface, and it's very diversified," Kessem noted, highlighting the ongoing challenge of protecting such wide-range information.

According to Kessem, cyberattacks and ransomware groups are becoming increasingly adept at infiltrating organizations. "They do it all day, every day, all day. They know everybody's network. Sometimes they sit in networks for a while and they watch everything," she said. Kessem emphasized the importance of organizations working with law enforcement when breaches occur, as it can significantly reduce costs and containment time.

Kessem's report highlights that organizations engaging law enforcement during ransomware attacks saved \$470,000 on average and reduced the containment period by 33 days. Despite these benefits, 33% of ransomware victims do not contact authorities and, as a result, they lose valuable time and resources.

Detection of breaches remains a challenge across all sectors; one out of three breaches are identified by the organizations' security teams, discovered by third parties, or informed by the cyberattack perpetrators. Kessem stressed that healthcare organizations, in particular, need to adopt comprehensive strategies to protect all types of patient data, including images.

High engagement from top leadership is crucial for effective cybersecurity. Organizations with proactive executive teams driving cybersecurity initiatives tend to better protect data. Kessem said, "When they engage and take on cybersecurity projects, you see participation and hard work from senior management teams. So, it's not just left just to the technical teams."

References:

Snowbeck, C. (2024, July 16). *Cyberattack costs growing at UnitedHealth Group, but profit still better than expected*. The Minnesota Star Tribune. <https://www.startribune.com/unitedhealth-cyberattack-change-healthcare-costs-profit/600381047?ref=metacurty.com>

Southwick, R. (2023, July 24). *Average cost of healthcare data breach rises to nearly \$11M*. Chief Healthcare Executive. <https://www.chiefhealthcareexecutive.com/view/average-cost-of-healthcare-data-breach-rises-to-nearly-11m>

To read the *The Minnesota Star Tribune* article, [click here](#).

To read the *Chief Healthcare Executive* article, [click here](#).



Bridgette Brashear

Senior Director
713-350-3321

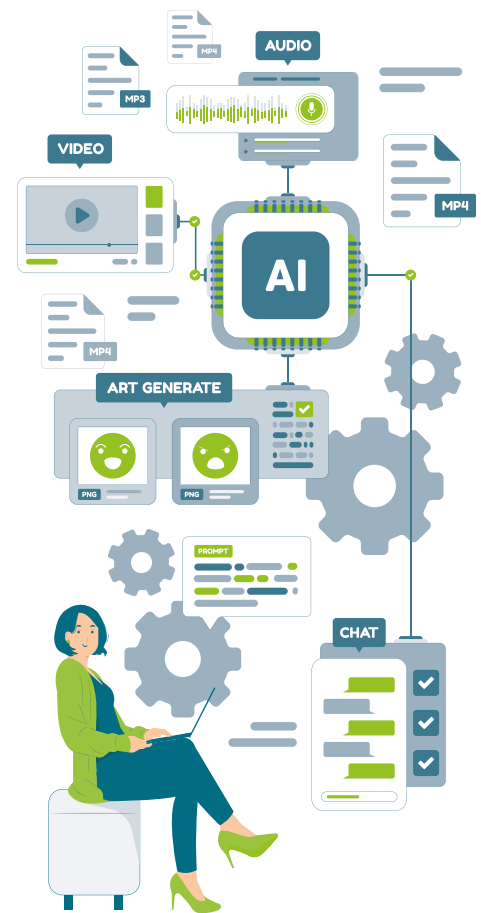
bridgette.brashear@alliantgroup.com
www.alliantgroup.com

What Is Generative AI?

Generative artificial intelligence (AI) is a subset of AI that refers to models and systems capable of generating new content, such as text, images, music, videos, and more. Compared to traditional AI, which primarily focuses on recognizing patterns and making decisions based on existing data, generative AI creates new data by learning from vast collections of data, and produces outputs that mimic human creativity.

Generative AI uses large language models (LLMs) to perform tasks that involve natural language understanding and generation. LLMs are trained on large amounts of data to recognize patterns, structures, and relationships within the

data. For example, text-based LLMs might be trained on books, articles, and websites. As LLMs process the data, they learn how words are typically used together, how sentences are formed, and the context in which certain phrases make sense, which is crucial for generating coherent text. Once the LLMs are trained, they can use what they learned to create new content, such as essays and stories. In short, LLMs are prediction engines that can guess the next words in sentences based on what came before them to finish sentences and paragraphs. LLMs are a key component of generative AI, enabling them to produce human-like text and perform a wide range of tasks.



Applications and Examples of Generative AI



CONTENT CREATION

- **Text Generation:** Certain models, such as ChatGPT by OpenAI, can write articles, generate poetry, create dialogue, and draft emails.
- **Image and Art Synthesis:** Tools like DALL-E 3 and Midjourney can create new images from textual prompts, which can be useful for design and the entertainment industry.
- **Music:** Some models, such as Suno, can compose music for creators.



ENHANCE DATA

- **Data Augmentation:** Generative AI can create additional training data for machine learning models, improving their performance without requiring more real-world data.
- **Simulation and Modeling:** It can generate realistic scenarios training autonomous systems, such as self-driving cars, in a virtual environment.



HEALTH CARE

- **Drug Discovery:** AI can generate molecular structures with potential therapeutic effects, accelerating the drug discovery process.
- **Medical Imaging:** Generative models can enhance the quality of medical images and assist in diagnostics by creating synthetic images for rare conditions.

Continued on page 6

What Is Generative AI? (Continued from page 5)

Free AI Courses

Amazon provides free AI and generative AI courses, ranging from the foundations to more technical information.

NONTECHNICAL AUDIENCES

Introduction to Generative AI: Art of the Possible provides an introduction to generative AI, use cases, risks and benefits.

[LEARN MORE >](#)

explore.skillbuilder.aws/learn/course/external/view/elearning/17176/introduction-to-generative-ai-art-of-the-possible



explore.skillbuilder.aws/learn/course/external/view/elearning/11322/introduction-to-machine-learning-art-of-the-possible



Introduction to Machine Learning: Art of the Possible is a course to help decision makers understand the fundamentals, benefits and risks of machine learning.

[LEARN MORE >](#)

Generative AI Learning Plan for Decision Makers is a three-course series covering how to plan generative AI projects and build generative AI-ready organizations.

[LEARN MORE >](#)

explore.skillbuilder.aws/learn/public/learning_plan/view/1909/generative-ai-learning-plan-for-decision-makers



DEVELOPER AND TECHNICAL AUDIENCES

explore.skillbuilder.aws/learn/course/external/view/elearning/17763/foundations-of-prompt-engineering



Foundations of Prompt Engineering introduces the basics of prompt engineering, the practice of designing inputs for generative AI tools, all the way to advanced prompt techniques.

[LEARN MORE >](#)

Low-Code Machine Learning explores how to prepare data, and train and deploy machine learning models with minimal coding and without requiring deep knowledge of machine learning.

[LEARN MORE >](#)

explore.skillbuilder.aws/learn/course/external/view/elearning/17515/low-code-machine-learning-on-aws



Continued on page 7

(Continued from page 6)

Google also offers a free course, **Beginner: Introduction to Generative AI Learning Path**, which provides an overview of generative AI fundamentals, including responsible AI principles.

[LEARN MORE >](#)

cloudskillsboost.google/paths/118



Ethical and Practical Considerations

While generative AI holds tremendous potential, it raises several ethical and practical concerns. With the ability to generate realistic text, images, music and videos, generative AI can be exploited to create fake news and other forms of misinformation.

Generative models can perpetuate and amplify existing biases present in training data, leading to unfair and discriminatory outcomes.

There is also the problem with intellectual property. Creating new content based on existing works

raises questions about ownership and copyright infringement.

Generative AI represents a significant leap forward in AI's capabilities, blending the lines between human creativity and machine intelligence. As it continues to develop, it promises to transform a wide range of industries, from entertainment to health care, by offering new possibilities and challenges in equal measure.

References:

Gewirtz, D. (2023, November 13). *I spent a weekend with Amazon's free AI courses, and highly recommend you do too*. ZDNET. <https://www.zdnet.com/article/unlock-ai-secrets-transform-your-skills-with-amazons-free-ai-learning/>

Ortiz, S. (2024, April 23). *What is generative AI and why is it so popular? Here's everything you need to know*. ZDNET. <https://www.zdnet.com/article/what-is-generative-ai-and-why-is-it-so-popular-heres-everything-you-need-to-know/>

Stryker, C., & Scapicchio, M. (2024, March 22). *What is generative AI?* IBM. <https://www.ibm.com/topics/generative-ai#:~:text=Generative%20AI%20excels%20at%20analyzing,smarter%2C%20data%2Ddriven%20decisions.>

To read the ZDNET article about Amazon's AI courses, [click here](#).

To read the ZDNET article about generative AI, [click here](#).

To read the IBM article about generative AI, [click here](#).



ZOOBOOK™
SYSTEMS LLC

Anna Komissarenko

President

800-995-6997

anna@zoobooksystems.com

AI Impacts Cybersecurity



It is important to be aware that as the use of generative artificial intelligence (AI) solutions increases, the risk of AI attacks also grows.

The U.S. Department of Health and Human Services, alongside its Health Sector Cybersecurity Coordination Center (HC3), released a briefing on AI and its impacts on cybersecurity in health care, as reported by *Healthcare IT News* (July 19, 2023). The briefing aims to help hospitals and healthcare organizations stay secure against AI-enhanced cyber threats. The report highlights risks posed by large language models (LLMs) such as ChatGPT, which can create convincing phishing emails and automate attacks. For instance, ChatGPT can generate emails with correct grammar and persuasive content, making the scams more believable and challenging to detect. The briefing also highlights an example of malware code that leverages Microsoft Teams for data theft and developer tools to infiltrate networks. HC3 recommends penetration testing, automated threat detection, continuous monitoring, cyber threat analysis, and AI training for cybersecurity staff. AI can also help detect and prevent cyberattacks by scanning emails and automating security tasks.

According to Netskope's *Cloud and Threat Report 2024*, users' adoption of generative AI solutions has seen rapid growth from 2% prior to 2023 to 10% as of November 2023. The notable increase in the use of ChatGPT, Grammarly, and Google Bard (now called Gemini) underscores the urgent need to address potential risks associated with these technologies, according to *KnowBe4* (January 24, 2024).

Cyberhaven, a data security services company, detected confidential data input into ChatGPT from 4.7% of 1.6 million workers at its client organizations, as the company reported in a blog (February 28, 2023). Examples include an executive who copied and pasted the company's 2023 strategy document into ChatGPT to generate a PowerPoint presentation and a doctor who input sensitive information into a letter that was sent to the patient's insurance company.

Employees are entering sensitive business and privacy-protected data into LLMs, risking that AI services might incorporate this information into their model training. Without proper data security, this data could be retrieved later, which can lead to potentially severe consequences such as financial loss, reputation damage and legal implications.

Continued on page 9

(Continued from page 8)

While AI poses a risk, it can also be a powerful tool for improving cybersecurity. AI tools can also aid in cyber education and prevention, automating security tasks and scanning emails for threats. AI models can learn normal behavior within an organization and help detect unusual behaviors, providing a strong defense against cyberattacks.

References:

Artificial Intelligence, Cybersecurity and the Health Sector. (2023, July 13). HHS. <https://www.hhs.gov/sites/default/files/ai-cybersecurity-health-sector-tlpclear.pdf>

Coles, C. (2023, February 28). *11% of data employees paste into ChatGPT is confidential.* Cyberhaven. <https://www.cyberhaven.com/blog/4-2-of-workers-have-pasted-company-data-into-chatgpt>

Fox, A. (2023, July 19). *HC3 warns about AI's cybersecurity impacts.* Healthcare IT News. <https://www.healthcareitnews.com/news/hc3-warns-about-ais-cybersecurity-impacts>

Sjouwerman, S. (2024, January 24). *Use of Generative AI Apps Jumps 400% in 2023, Signaling the Potential for More AI-Themed Attacks.* KnowB4. <https://blog.knowbe4.com/use-of-ai-apps-jumps-400-in-2023-signaling-more-ai-themed-attacks>

To read HC3's *AI, Cybersecurity and the Health Sector* briefing, [click here](#).

For further information about Cyberhaven's analysis, [click here](#).

To read the full *Healthcare IT News* article, [click here](#).

To read the full *KnowBe4* article, [click here](#).

Use of Generative AI in New Jersey



Generative artificial intelligence (AI) has the potential to transform state government. Still, it must be implemented responsibly and with proper oversight, according to Chris Rein, New Jersey Chief Technology Officer, in a recent *Statescoop* interview (May 14, 2024). He emphasized the need to balance the benefits and risks of generative AI and highlighted the importance of legislation to protect data privacy. Rein mentioned the promise of improved services through AI while ensuring the responsible use of residents' data. He aims to finalize a report from the Governor's AI Task Force, established in late 2023, to provide guidelines for AI use in New Jersey and plans to collaborate with the State Legislature and governor's office to fund and regulate the AI initiatives.

To read the original article, [click here](#).

Future-proof your New Jersey agency with an EHR experience that's uniquely yours.

140+ New Jersey agencies trust Qualifacts because of our award-winning behavioral health EHRs and deep understanding of your billing and reporting requirements.

Learn More:



QUALIFACTS™

Spyware on Phones: Know its Impacts and Delete It

Spyware is malicious software that enters users' computers to gather data and sends it to third parties without contest. However, it is not just a problem for personal computers; it can also affect mobile devices. Mobile spyware can disguise itself as fake applications or corrupt current legitimate ones, turning them into data stealers, as explained by *ZDNET* (May 30, 2024). Remote monitoring applications meant for personal or work use can be misused to invade privacy. Mobile spyware can steal information, track locations, record conversations, and more.

Forms of Spyware

There are many forms of spyware, and understanding their basic differences is crucial before undertaking the problem.



Nuisanceware is a type of software that often comes bundled with legitimate applications and primarily aims to disrupt users' experience for profit. Examples include:

- **Pop-up ads:** Interrupting web browsing with frequent and intrusive advertisements
- **Browser hijacking:** Changing the homepage or search engine setting without permission
- **Data collection:** Gathering browsing data to sell to advertising agencies and networks

While nuisanceware is generally not considered a direct threat to a system's core security, it focuses on generating illicit revenue by creating forced ad views and clicks. It is often categorized as a form of malicious advertising due to its intrusive nature and the way it manipulates the browsing experience.

1

Continued on page 11

(Continued from page 10)

Standard mobile spyware steals operating system and clipboard data, cryptocurrency wallet information, and account credentials. It can be spread through phishing, malicious email attachments, social media links and fraudulent text messages.

2

Advanced spyware, also known as **stalkerware**, is more sophisticated and unethical, and commonly found on phones. Unlike basic spyware, stalkerware often includes invasive and persistent features, which make it more dangerous. Key characteristics include:

3

- **Data Theft:** It can steal detailed personal information, such as financial data, account credentials, emails, and messages.
- **Location Tracking:** It can track devices' physical locations, compromising users' privacy and security.
- **Surveillance:** Advanced spyware can enable unauthorized access to devices' microphones and cameras, allowing real-time eavesdropping and recording.
- **Stealth and Persistence:** It often operates undetected, using sophisticated methods to hide its presence from standard security measures. It can survive system reboots and attempts to remove it, often requiring specialized tools for complete removal.

Government-grade commercial spyware refers to highly sophisticated surveillance software developed by private companies and sold to governments and other authorized entities. This type of spyware is designed to covertly infiltrate and monitor electronic devices to gather intelligence, track activities, and intercept communications. A well-known spyware used by various governments is Pegasus, created by NSO Group to combat terrorism. Key characteristics include:

4

- **Advanced Capabilities:** This spyware includes features such as keylogging, screen capture, microphone and camera activation, GPS tracking, and the ability to intercept and decrypt communications.
- **Stealth and Persistence:** It is designed to operate undetected, often evading detection by antivirus software and other security measures. Once installed, it can remain on devices for extended periods of time while continuously gathering data.
- **Exploitation of Vulnerabilities:** This spyware often exploits zero-day vulnerabilities—undisclosed software flaws that provide backdoor access into systems.
- **Legal and Ethical Concerns:** The use of this spyware raises significant privacy and human rights issues, particularly when governments employ it to monitor journalists, activists, and political opponents.

While government-grade commercial spyware is a powerful tool used for surveillance with legitimate applications in national security, it can also be used against civil liberties.


Continued on page 12

Spyware on Phones: Know its Impacts and Delete it

(Continued from page 11)

Detecting Spyware

There are several signs that can indicate the presence of spyware on phones.

- 
- 1

Unusual Battery Drain
 Spyware can run constantly in the background, leading to significantly faster battery depletion.
 - 2

Overheating
 A phone that becomes unusually hot, even when not in use, could be running spyware or other intensive background processes.
 - 3

Increased Data Usage
 Spyware often sends data back to its controller. Unexplained spikes in data usage can be a red flag.
 - 4

Strange Behavior
 Unexpected reboots, crashes, and slow performance can be signs of spyware. In addition, applications may also open and close on their own.
 - 5

Background Noise
 Unusual sounds and static during phone calls can sometimes suggest the microphones are being used for eavesdropping.
 - 6

Unfamiliar Apps
 Check for rogue applications that may have been installed.
 - 7

Unusual Text Messages
 Receipt of strange text messages with random characters, symbols and/or codes can be attempts by spyware to communicate with its controllers.
 - 8

Pop-ups and Ads
 Frequent pop-ups and ads that appear even when users are not browsing the web may be a sign of spyware.
 - 9

Delayed Shutdown
 If a user's phone takes longer than usual to shut down, it might be because spyware is running in the background.
 - 10

Security Warnings
 If a user's phone or antivirus flags unusual activities, take it seriously.

Continued on page 13

(Continued from page 12)

What Do You Do about Suspected Spyware?

■ Run Security Scans

Use reputable antivirus or anti-spyware applications to scan for and remove malicious software.

■ Update your Phone Operating System

Ensure your phone has a current operating system. Updates often include security patches.

■ Check Application Permissions

Review the permissions of installed applications and revoke any unnecessary and suspicious permissions.

■ Consult a Professional

If you are unsure or need help, consider seeking assistance from a cybersecurity professional.

■ Complete a Factory Reset

As a last resort, a factory reset can remove spyware, but be sure to be back up important data first because the reset will erase all data from the phone. Note that sophisticated spyware can sometimes survive a reset.

- For Android users, go to Settings, General Management, Reset, and then Factory Data Reset. For further information on how to reset and backup Android devices, [click here](#).
- For iPhone users, go to Settings, General, Transfer or Reset phone. For more information on how to reset and back up data, [click here](#).

Reference:

Windsor, A. (2024, May 30). *How to find and remove spyware from your phone*. ZDNET. <https://www.zdnet.com/article/how-to-find-and-remove-spyware-from-your-phone/>

To read the full ZDNET article, [click here](#).



Jon Trigg

SVP, Sales & Marketing
jtrigg@coresolutionsinc.com
(610) 687-6080



**TECH
MERCENARIES**

Call Rob Molinaro for all your data and telecommunication needs.
Tell him that the IT Project referred you!
(610) 608-0127
Rmolinaro@techmercenaries.net



Jawad Sartaj

CEO
Jawad.Sartaj@Informd.ai
(917) 681-4560

Tristan Keelan

Director of Development
and Growth
tkeelan@informd.ai
(716) 427-9911

informd.ai



**VIDERA
HEALTH**

Genevieve Longtin

Director of Marketing
genevieve@viderahealth.com
(833) 401-2231
viderahealth.com

Copilot: Microsoft 365 Chatbot and Ways to Use It

According to P. Gralla, (7 ways to use Microsoft Copilot right), Microsoft Copilot is a conversational interface that enables users to search information, generate text to summarize websites, and write emails. It also generates images using prompts. Users can even ask to write code in various computer languages, such as JavaScript, C, and Python. Copilot uses large language models (LLMs) to do its work and is based on Open AI's GPT-4 model.

Copilot for Microsoft 365 became available for all users on November 1, 2023, and offers a free subscription option.

- **Copilot Free:** This version allows users to chat using text, voice, and images. It can also summarize documents and web pages, create images, and use plugins.
- **Copilot Pro:** Currently priced at \$20 per user/month, this version includes everything in the free version plus faster response and image creation during busy hours. Copilot is also available in select Microsoft 365 applications.
- **Copilot for Microsoft 365:** This version is for businesses and is available at \$30 per user/month. It includes Copilot in Word, Excel, PowerPoint, OneNote, Outlook, and Microsoft Teams.



How to Access Copilot

1. Windows 11 Taskbar Shortcut:

- In Windows 11, users can launch Copilot by clicking on the 'Copilot' icon on the taskbar or using the Windows key + C shortcut.

2. Copilot App:

- Install the Copilot application to a phone or computer.

3. Web Access:

- Microsoft Edge has Copilot ready on the navigation pane. If the user is not already logged in, signing in to Microsoft365.com will be required.
- If the user does not have Microsoft Edge, Copilot can still be accessible through Bing, and sign-in is not required.

4. Microsoft 365 Apps:

- If the user has a subscription, Copilot can be used in Word, Excel, PowerPoint, Outlook, and Teams.

Continued on page 15



Sherry Marchand, CPMA
 Founder and Senior Consultant
 540-660-1733
 smarchand@coresolutions.biz



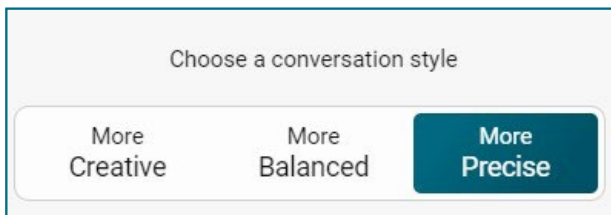
Mike Underwood
 Director, Integrated Marketing,
 Communications
 and Brand Strategy
 609-759-5096
 munderwood@ixpcorp.com
 www.ixpcorp.com

(Continued from page 14)

Ways to Explore the Free Version of Copilot

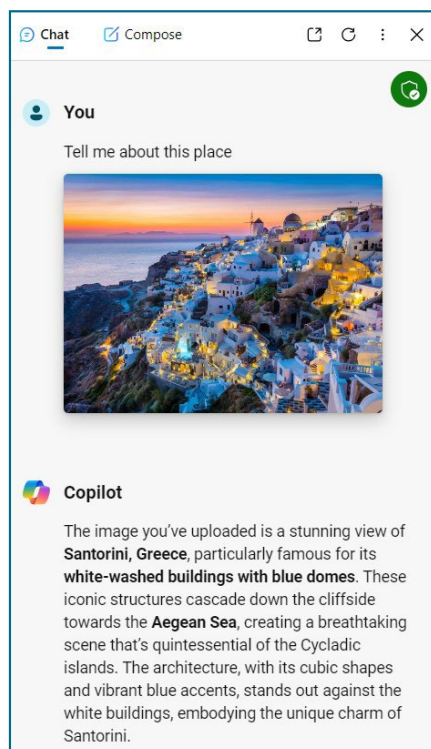
1. Have a conversation

There are three chat modes: Creative, Balanced, and Precise. Pick one to have a more customized response. Microsoft also recommends avoiding relative terms and instead, using specific words when asking questions and writing prompts.



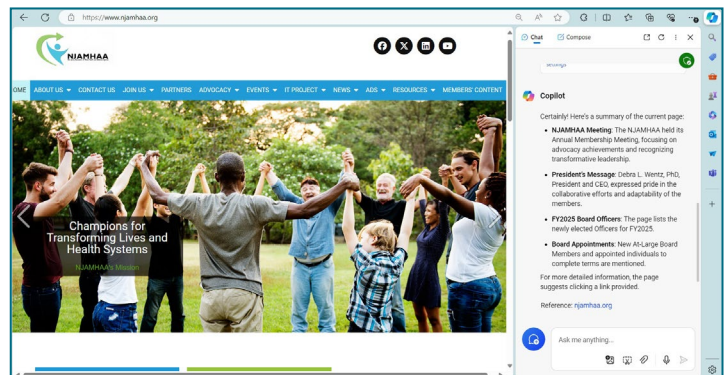
- Creative mode creates more imaginative responses, which are best for finding inspiration, brainstorming ideas, and doing creative writing.
- Balanced mode delivers more engaging and informative responses.
- Precise mode provides right-to-the-point answers that do not include any unnecessary words or information.

Users can also use text and images to interact with Copilot simply by dragging an image from the web or a computer and asking related questions.



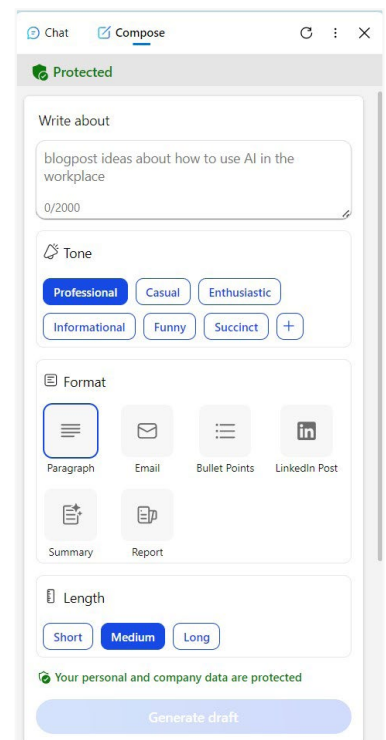
2. Create a web page or article summary

Click on the Copilot icon in the upper right corner of the Microsoft Edge navigation; then click on the 'Generate page summary' button. If the user does not have Microsoft Edge, this action can still be done through Bing by asking the search engine for a key point or summary of a web page and pasting the URL.



3. Draft Content

Copilot can help draft various content, such as emails, stories and poems. It can also help code programs and more. For better results, users should be specific and provide detailed guidelines. When launching Copilot in Microsoft Edge, choose 'Compose' on the top tab. In this section, users can describe what the draft can be, select which tone works, what format it is going to be (e.g., paragraph, email, bullet points, or social media post), and the length of the content it needs to generate.



Continued on page 16

Copilot: Microsoft 365 Chatbot and Ways to Use It

(Continued from page 15)

Always Double Check

While using Copilot, just like all generative AI, always review the generated content since AI systems can produce errors, glitches, and incorrect code and text. Chatbots tend to make things up or to 'hallucinate'. As IMB describes it on its website, "AI hallucination is a phenomenon wherein a large language model (LLM)—often a generative AI chatbot or computer vision tool—perceives patterns or objects that are nonexistent or imperceptible to human observers, creating outputs that are nonsensical or altogether inaccurate."

Adapted with permission from:

Gralla, P. (2024, January 22). *7 ways to use Microsoft Copilot right*. Computerworld. <https://www.computerworld.com/article/1611598/7-ways-to-use-microsoft-copilot-right.html>

To read the full *Computerworld* article, [click here](#).



Neal Wexler
Director of Sales
516-986-9552
neal.wexler@accumedic.com



Gerry Blass
President & CEO, ComplyAssistant
800-609-3414 Ext 700
www.complyassistant.com



Jannel Alston
Project Manager, Marketing
jannel.alston@therapybrands.com
205.941.6886
therapybrands.com



Sandra Rocha-Bucco
Client Development Executive
908.347.1317
srocha@ntst.com

Make the most of your NJAMHAA membership!

Participate in NJAMHAA's practice groups!

Staff from all member organizations can participate in our groups.



Information Technology (IT) Practice Groups

■ Billing Supervisors Practice Group:

Improves the way NJAMHAA member agencies bill and collect for services rendered; addresses billing issues relating to the Health Insurance Portability and Accountability Act (HIPAA), Medicaid and other third-party billing entities; provides analysis, support and advocacy.

Meeting date: February 20, 2025 10:00 A.M. to 11:30 A.M.

■ Human Resources (HR) Practice Group:

The IT Project has expanded the scope of compliance to human resources since this business unit also has regulatory issues where the use and implementation of technology can assist. This group often has subject matter experts to present to the committee regarding best practices, regulatory compliance and avoiding HR pitfalls when working with their employees.

Meeting dates:
March 20, 2025 10:00 A.M. to 11:30 A.M.
June 12, 2025 10:00 A.M. to 11:30 A.M.

■ IT Professional Advisory Committee:

The IT PAC plays an integral role in the advocacy efforts of the IT Project for member agencies' IT needs; assists behavioral healthcare providers in the collection, processing, integration and interpretation of data through automation; shares technical expertise, future trends and the management of outcome, performance and financial data; and investigates the application of new technologies to increase efficiency, enhance revenue, reduce costs and improve quality of services.

Meeting date: March 17, 2025 10:30 A.M. to 12:00 P.M.

■ Quality Assurance/Compliance Practice Group:

This group shares information about quality assurance/performance improvement, licensing, regulations, standards, accreditation, corporate compliance and more.

Meeting date: January 23, 2025 10:00 A.M. to 11:30 A.M.

To join any of these groups, please contact Shauna Moses, Vice President, Public Affairs and Member Services at smoses@njamhaa.org.

Please also contact Shauna if you need additional information.

IT Project Services

- Group Purchasing discounts for hardware and software, industry events, publications, marketing services, and more
- Vendor User Group promotion and facilitation
- Grants facilitation and access to philanthropic donations; resources reported regularly via *Newswire*, NJAMHAA's tri-weekly electronic newsletter, and e-blasts.
- Partnerships with state and local government entities, e-learning companies, benchmarking firms, and leading technology vendors provide access to an array of products and services.
- Annual Technology Conference presents the latest information on popular trends and emerging technologies; first-hand information about non-profit policy and funding issues and regulatory mandates; and opportunities to network with top technology companies.
- *Bits & Bytes* biannual newsletter highlights IT Project activities, product evaluations, industry surveys, vendor news, case studies, technology tips and techniques, grant information, and much more.
- Consultation services for electronic health record implementations
- Expert technical support and network engineering services available at below-industry market rates
- LAN/WAN/VPN, VoIP, Disk to Disk backups and Internet Monitoring solutions
- Managed services for all your circuits, servers and desktops
- Technology plan development
- Assistance in purchasing technology solutions
- Compliance assistance (federal and state, as related to privacy and security)
- Grant and product donation information
- Additional training, through workshops and webinars

BUNDLED SERVICES

Block of 200 Hours:
\$18,068.00 (\$90.34/hour)

Block of 100 Hours:
\$9,251.00 (\$92.51/hour)

Block of 75 Hours:
\$7,448.00 (\$99.31/hour)

Block of 50 Hours:
\$5,416.00 (\$108.33/hour)

If you are interested in our rates for a block of time of more than 200 hours or fewer than 50 hours, please contact

Ron Gordon
Director, IT Project
RGordon@NJAMHAA.org



“I wanted to thank NJAMHAA for putting together and hosting such an amazing conference. The importance of IT in mental health services delivery could not be overstated and this conference successfully demonstrated the potential for collaboration among providers to improve mental health outcomes for patients.”

Bonny Uchenna Life, PhD, MA, MPP

Program Director, DD Services - CARES, Behavioral Health and Psychiatry, Trinitas Regional Medical Center



Technical Assistance and Consulting

specializing in non-profits at below-market rates

Microsoft 365 Implementation & Management:

Microsoft offers it all for free to all 501(c)(3) non-profits

The IT Project can help you with ordering and implementing Microsoft 365 for your organization.



Technical liaisons between you and your IT vendors



Cloud implementation and conversions



HIPAA/HITECH compliance resources and e-book for sale, \$800 discount off retail

Configuration and maintenance of:

- Microsoft Cloud Entra/Azure
- Cloud Virtual Servers
- Virtual Private Networks (VPN)
- Local Area Networks (LAN)
- Wide Area Networks (WAN)

Vetted vendor relationships that can SAVE YOU MONEY!

- Telecommunications - VoIP and Cellular
- Security audits
- Penetration testing
- Hardware and software purchases
- Electronic health record vendors



For information on how the IT Project can help you, contact:

Ron Gordon
Director, IT Project

609-838-5488 x 215
rgordon@njamhaa.org





Procentive

Powered by **Therapy** Brands

Maximize Efficiency and Revenue:

Exclusive EHR + Managed
Billing Bundle Offer!

**50%
OFF**

the first 3 months
of Procentive when
bundled with
managed billing.*

WHY PROCENTIVE EHR?



Easier Documentation

Utilize pre-written treatment plans
and customizable templates.



Efficiency Tools

Integrated billing, eMAR,
custom forms, CC processing,
integrated fax, and more!

WHY MANAGED BILLING?



Faster Payments

Streamline your billing process
and get paid quicker.



Expert Management

Our RCM team collaborates
with you to address your
unique challenges.

* Offer applies exclusively to Procentive when bundling EHR and RCM services. A 36-month contract is required.
Discount applies only to the first 3 months of Procentive subscription.