

# DELAWRITER

The quarterly newsletter of AMWA-DVC

Indian Summer, 2022

## **AMWA-DVC Holiday Meeting & Networking Events** *Stay tuned for information about our January 2023 Holiday event!*

### **Virtual Holiday Meeting & Networking on January 5, 2022**

Jolly attendees – some in Santa or elf hats and draped in tinsel – enjoyed a bit of cheerful socializing before Laura Ninger, ELS, President of Ninger Medical Communications, LLC, delivered a presentation entitled “Habits of Highly Effective Medical Writers.” Members then broke into smaller groups to discuss best work habits and writing practices. Group topics included writing/researching, editing/proofreading, bookkeeping, marketing, or open networking. Raffle prizes and networking opportunities were enjoyed by all.



### **How Pivots in Life Can Lead to a Successful Freelance Business**

*by Viola Brown*

A wide variety of presentations were on offer at the AMWA-DVC 20th Annual Freelance Workshop, held virtually on March 12, 2022. The keynote speaker was Brian Bass, MWC, President of Bass Global, Inc., who presented "Pivoting to Thrive in Your Freelance Medical Writing/Editing Business." The topic's focus was decisions that can help propel our freelance careers in medical communications. But he began, by way of contrast, with what he regards as his two most ill-considered decisions. The first was leaving an advertising writer position in New York City due to the long commute from New Jersey and the long hours. Although Bass had accepted a job offer closer to home, prior to finalization the hiring company informed him that the New Jersey location was closing, and he would need to relocate. The second ill-considered decision was spending a week pondering; although it was important to make the best decision for himself and his family, he also used this time to try freelancing. In the interim, the company rescinded its job offer – leaving him unemployed. Bass explained that he

refused to let this incident deter him and chose to continue leveraging his writing experience to work freelance. Later, he joined a small advertising agency and wrote pieces in the field of animal pharmaceuticals. There, Bass learned medical writing and valuable business principles, which helped him promote his business and gain confidence.

Of course, challenges arise for freelance medical writers, too. Perhaps one of the most potentially expensive difficulties Bass faced was non-payment (six figures) by a long-standing client. Instead of taking the client to court, he established a new contract to schedule regular client payments and help them manage the debt. More importantly, Bass institutionalized checks and balances in Bass Global, Inc.'s contracts to help prevent such occurrences in the future. **The valuable lesson:** It is our responsibility to ensure that our business finances are not neglected, and non-paying clients should be confronted sooner rather than later.

Bass shared another lesson learned through experience. A medical communications agency he had joined failed to communicate regularly with a client despite an approaching Prescription Drug User Fee Act (PDUFA) product-launch deadline. Although it was not his responsibility, Bass maintained contact with the client. The agency eventually cut off all communication with the client, but Bass worked 72 hours — with no payment — to help the client meet their PDUFA deadline. Years later, this same client remembered how his intervention saved their product launch, and they reached out to Bass Global, Inc. to update their medical materials. **The valuable lesson:** Being willing to help and going the extra mile creates good will and, often, extra business.

“Breaking into freelance medical writing takes patience. It took me about 7 to 8 years to develop a sufficient client list and not have to market traditionally,” Bass said. Along with the challenges, however, are personal, professional, and financial rewards. “But keep in mind,” Bass noted, “that freelancers generally experience more stress in their work than employees.” Therefore, growing a business too big can have limited benefits as the balance between the pressures of growth and compensation changes. Only you can decide what is “too big.” If the benefits are fewer than the stresses, it is best to remain smaller. Growth will be advantageous if the stresses are equal to or fewer than the rewards.

Freelance medical writers make choices that are sometimes difficult, but necessary. “Choosing not to choose is a choice, not deciding is a decision, and all outcomes are out of your control. Whenever you are faced with a challenge, make a choice. Fear is the reason many people do not make choices, but do make that decision, no matter how hard it is. If you choose well, you will win. If you choose poorly, you will learn.” Learning is part of becoming a great freelance medical writer. We must employ principles learned and duplicate what works.

*Viola Brown is a recent graduate of Temple University's Professional Science Masters in Scientific Writing program. She aspires to write and edit publications and medical documents.*

---

## Cybersecurity Basics for Medical Writers

*by Katherine Molnar-Kimber, PhD*

The internet provides the infrastructure for rapid communication and international collaboration, which can benefit many medical writers. However, users need to remain vigilant.

The first ransomware attack occurred in 1989: a Harvard-trained biologist, Dr. Joseph Popp, mailed out 20,000 ransomware-infected disks to colleagues abroad from the WHO AIDS Conference with a title “AIDS Education Software.” The ransomware has been called the “PC Cyborg” and the “AIDS Trojan.” The disk also came with a warning, but some did not heed it. After insertion into the computer and 90 reboots, the infected computer stopped working. At first, scientists and clinicians needed to send a \$189 payment to PO Box in Panama to release a recovery program to unlock the computer. Ransomware has proliferated and evolved since then.[1,2]

A cybersecurity breach can come from anyone, including a colleague, a colleague's hacked email address, an almost identical-looking website to your financial institution's website, or an "invoice" from Quickbooks.[3] To avoid opening a colleague's hacked email, check the email address of each sender before opening.[3] If it is spam, consider putting the email in trash before opening because the unsubscribe link may contain malicious code.[3]

### Cybersecurity Vocabulary

**Data breach:** "serious adverse event" when information is stolen from a database without knowledge or permission of owner; often involves personal information (eg, credit-card information, birthdate, social security number) from many customers.

**Data blocker:** small piece of equipment that is placed between the charging device and your device. It prevents download of your data to a server and upload of any software or data onto your device.

**Firewall:** security device that acts as a gatekeeper and can be set to different protective levels. It monitors traffic and can block access to the computer's data from unrecognized sources.

**Malware:** software designed to gain unauthorized access and disrupt or damage a computer.

**Phishing:** fraudulent email pretending to be from reputable company to coerce individuals to reveal personal IDs.

**Ransomware:** form of malware that restricts access to your files and data by locking computer or encrypting files without your permission. Requests payment for key to unlock computer.

**VPN:** virtual private network establishes a secure connection between your computer and the internet, reducing tracking.

### Cybersecurity for business

Multiple layers of firewalls are recommended. A broadband router is an example of a hardware firewall.[4] A software firewall (program) monitors port numbers and applications on the computer. Cloud-based firewalls are often employed by multi-person businesses and can grow with the organization. Firewalls can also be described by their filtering capacity such as packet-filtering firewalls, proxy service firewalls, stateful multi-layer inspection (SMLI) firewalls, unified threat firewalls, network address translation (NAT) firewalls, and virtual firewalls.[4]

Antivirus and anti-malware software, even for Apple MACs, are highly recommended. Installing a VPN on your computer can limit tracking and vulnerability to hacking. [1,3] Updates of all software should be installed within 24 hours to reduce vulnerabilities of your computer.[3] Tip: Update all software before leaving on trip. (Caution: Do not accept any software updates at hotels, restaurants, or other public spaces.[3])

A back-up system helps protect against unexpected emergencies, such as fire. A separate back-up drive that is only attached during the backup process avoids having any malware loaded onto your back-up drive during your business day.

### Passwords and multifactorial authentication

If you use the same password for multiple accounts, then you potentially provide a master key to a hacker. Each password should be unique and contain a combination of at least 10-12 small letters, capital letters, numbers, and (when applicable) special characters. [1,3] Some experts recommend a phrase containing a combination of these elements. The password should not contain birthdays or birthdates; names of pets, children, or family members; or any characteristics that are described on your social-media posts. Some cybersecurity experts suggest using a password manager. [1,3,4] Others approve of an offline list of passwords.[3]

Many financial institutions and email services use questions (eg, favorite color, teacher,

first pet) to act as a confirmation of the person requesting access to the account. To maintain their usefulness, these answers should not appear on any social-media posts or platforms.[1,3] When these topics come up at networking events or parties, people should consider providing other answers than those used for the security questions.

Many websites protecting financial data use real-time multifactorial authentication to check the person's identity: a code is sent to an approved phone number or email address. This process is effective unless a hacker has usurped your phone number. [3] Consider setting up a security code with your mobile provider to block a hacker's ability to take control of your cell number.[3]

On a personal note, one subscription renewal service asked me for my eye color—I provided a rare color (magenta) since it was only being used for security. Thus, whenever a company asks for personal information to set up an account, consider whether they really need it. They may not.

Note that Who's Who often provides parents' names, including mother's maiden name, spouse's name, and children's names with birthdates, so if you're listed in Who's Who and banks ask to use your mother's maiden name, consider using the name of a different relative.

### **Additional considerations for freelance medical writers**

Providing information to clients about your bank account can provide bidirectional access.[1,3] Fees to third parties such as PayPal can be considered the cost of doing business because the third party shields your financial data (eg, credit cards and bank accounts) from the client.[1] Alternatively, some payment companies such as Bill.com protect the identity of your business account while allowing rapid payment from multiple clients without charging fees to the recipient.

Companies notice how you send your confidential EIN number and may assume your process reflects the handling of their confidential information. Transferring of confidential documents can be accomplished by confidential cloud-based storage systems such as your client's Dropbox folder, SharePoint, etc.

Encryption is available with MSFT 10 pro, Enterprise or Education, and Apple Fireball. [1] Encrypted email can keep your discussion of client data and strategies confidential. Proton mail ([www.protonmail](http://www.protonmail)) is an encrypted open-source email service housed and operated in Switzerland.[1] Email service with Hushmail.com has an option to encrypt any specific email; the service is located in Canada.

Because removing your browser history from your computer does not remove it from the browser, consider using Firefox with a search engine that does not save browsing history such as [www.duckduckgo.com](http://www.duckduckgo.com). [1,3]

### *Home office*

Reducing the number of insecure points of contact to your home office helps protect your system. While many people use several smart devices such as thermostat, voice command devices (eg, Alexa, Amazon fire stick), and doorbells at home, these devices are less secure than the computer.[1,3] To reduce the potential crossover of risk, consider having two internet connections—one for home office and a different one for home devices.[1] Alternatively, choose devices without the smart device features.

### *Cybersecurity on the road*

Cybersecurity on the road requires extra vigilance. Online privacy with a VPN can enhance cybersecurity so consider setting up a VPN on the laptop before traveling. Some patrons in open hotspots in hotels and restaurants may have software that can read others' computers in the area. Consider using a data blocker between the charger and your device to block the unintended reading of your data from your device at any facility beyond your home office.[3] As a precaution, consider removing any unnecessary confidential files (eg, those of other, non-trip-related clients) from the laptop before traveling.

Since a car (rental or your personal vehicle) can upload a phone's data, such as client communications, to the car computer,[1,3] consider charging your cell phone before getting in the car or alternatively, consider using a data blocker.

## Selected sources

- [1] Byram JK. Medical Writer's Guide to Cybersecurity. AMWA 2021 National Conference.
- [2] Simone A. The Strange History of Ransomware Floppy disks, AIDS research, and a Panama P.O. Box. <https://medium.com/@alinasimone/the-bizarre-pre-internet-history-of-ransomware-bb480a652b4b>  
Accessed April 3, 2022.
- [3] Lanza, J. "Cybersecurity: Simple Safeguards" Jan 27, 2022.  
Contact information: <https://thelanzagroup.com/>
- [4] Norton. What is a firewall? Firewalls explained and why you need one.  
<https://us.norton.com/internetsecurity-emerging-threats-what-is-firewall.html>  
Accessed September 2, 2022

*Katherine Molnar-Kimber, PhD, is the owner of KMK Consulting Services of Kinnar Group LLC in Worcester, PA and writes predominantly scientific publications, Continuing Medical Education Needs Assessments and programs, and white papers.*

---

## The Cholera Outbreak of 1854: John Snow Knows Something

by Sarah A. Broskin, MS

Soho, London in the late summer of 1854. The streets are nearly empty. A few people are removing bodies of the recently deceased from homes on almost every street. The groans of the dying can be heard through the open windows. Soho is in the midst of the worst cholera outbreak in years. Hundreds have died in the last week after suffering from severe bouts of vomiting and diarrhea. Those who haven't contracted the illness are fleeing London in droves.

Physicians tending to the ill and dying know the pattern all too well: rotting organic matter or *miasma* has polluted the air causing an epidemic. The same "bad air" is thought to be responsible for prior chlamydia and bubonic plague outbreaks. The cholera outbreak in Soho has been particularly bad due to the high amounts of *miasma* coming from the nearby Thames River. The stagnant, foul smelling air is impossible to escape in Soho. The only hope for residents to combat *miasma* is to limit exposure to foul air and to excessively wash their bodies. Everyone is following this guidance, with the exception of one person: John Snow.

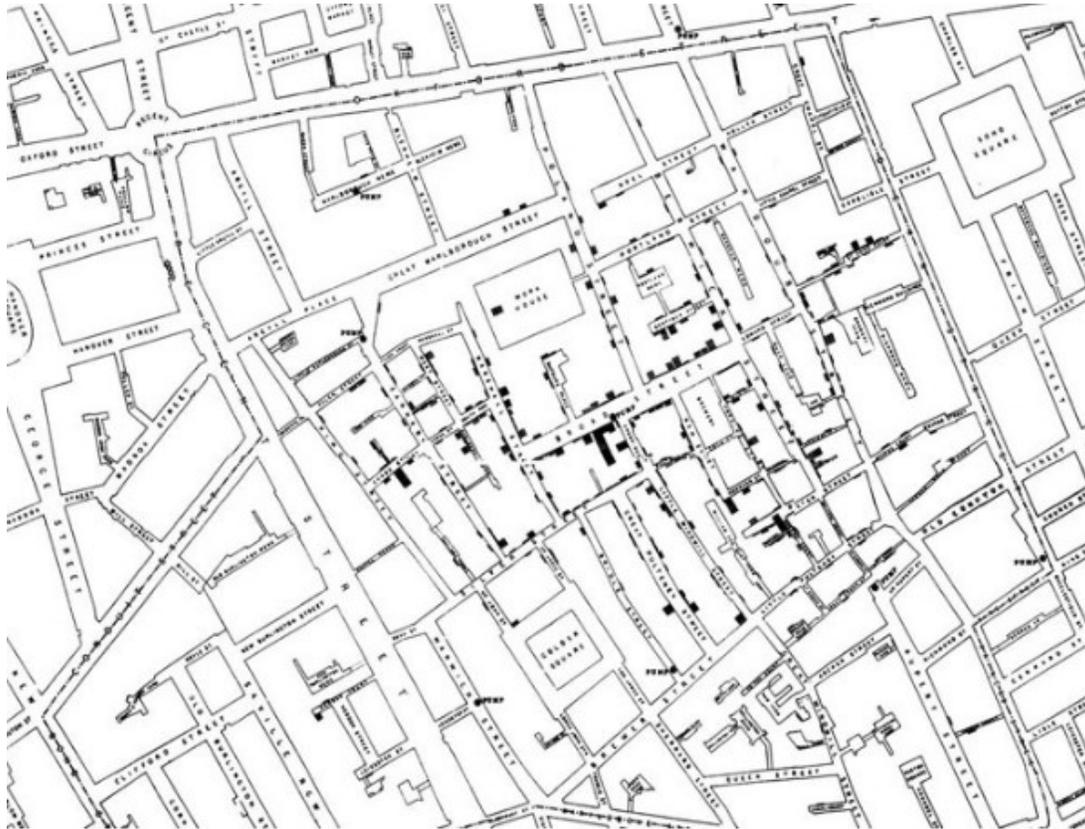
Snow is a physician and a resident of Soho. He is well known in the medical community for his work on ether and chloroform as forms of surgical anesthesia. Lately, however, John Snow has been combing the streets of Soho, trying to track down the source of the cholera outbreak. Rumors are spreading that Snow doesn't agree with the prevailing *miasma* theory. Snow believes another mechanism is contributing to the quick spread of this cholera outbreak other than "bad air."

By talking to residents, Snow makes a crucial observation: those households most impacted by cholera share one thing in common, their water source. Most residents of the area obtain their water from the Broad Street pump. Snow confirms his theory by talking with the local brewers, who have largely been spared from the cholera outbreak. Although the brewery is located near the Broad Street pump, the brewers only drink from a different water pump located within the brewery. Snow checks the water from both sources, but can find no signs of contamination. Yet his observations are strong enough to persuade local authorities to remove the handle of the pump, ending the cholera outbreak as quickly as it started.

John isn't done, however. His scientific mind can't let go of the need to understand what the mechanism is behind the spread of cholera. John maps the cholera outbreak, further linking the association of cases with the Broad Street pump. As another outbreak begins, John intensifies his investigation. Suspecting water transmission, John maps cholera cases by household location. He discovers that two water systems supply homes in the area: one upstream of the Thames River in an area with less polluted water and one downstream in an area of the river highly polluted by sewage. The polluted, downstream supply of water is linked with over ten times the number of cholera deaths as the upstream supply. This evidence supports John's hypothesis that the source of cholera is contaminated water from the Thames River, not just "bad air."

**John Snow's map of the cholera epidemic in London changed how we**

interpret infectious disease and provides a model to track outbreaks.



Sarah Broskin, MS completed her certificate in Scientific Writing at Temple University, College of Science and Technology. She has extensive experience as a bench scientist in oncology and currently works at Janssen Pharmaceuticals R&D. She looks forward to a career in scientific writing and medical communications.

**2022**  
**AMWA**

Medical Writing & Communication Conference  
NOVEMBER 2-5, 2022  
DENVER, CO

*Trends and Opportunities for Medical Communicators*

**Elevating health and well-being through medical communication.**

**REGISTER NOW!**

# Dinner in Denver

Chapter Networking Dinner on Thursday, November 3 during AMWA's Annual Meeting in Denver, Colorado



## Quotable quotes from notable folks

Carl Sagan



1934 - 1996

"We live in a society exquisitely dependent on science and technology, in which hardly anyone knows anything about science and technology."  
— Carl Sagan

Stephen Hawking



1942 - 2018

"Not only is it important to ask questions and find the answers, as a scientist I felt obligated to communicate with the world what we were learning."  
— Stephen Hawking

Neil deGrasse Tyson



1958 -

"The good thing about science is that it's true whether or not you believe in it."  
— Neil deGrasse Tyson

## Delawriter Editorial Team

The *Delawriter* is published quarterly by the American Medical Writers Association-Delaware Valley Chapter

Executive Editor: Helen Fosam, PhD

Editor: Katherine Molnar-Kimber, PhD, and incoming Delawriter Editor Jacqueline M. Mahon, MA

Designer: Darryl Z. L'Heureux, PhD

Editorial Consultants: Elisha Gillette and Robert Hand, MSc

Please direct change of address/information to AMWA Headquarters Staff:

American Medical Writers Association

30 West Gude Drive, Suite 525

Rockville, MD 20850-1161

(240) 238-0940 (telephone)

(301) 294-9006 (fax)

email: [amwa@amwa.org](mailto:amwa@amwa.org)

Visit our AMWA-DVC website

AMWA-DVC | AMWA National, 30 West Gude Drive, Suite 525,  
Rockville , MD 20850

[Unsubscribe membercommunications@amwa-dvc.org](mailto:membercommunications@amwa-dvc.org)

[Update Profile](#) | [Constant Contact Data Notice](#)

Sent by [membercommunications@amwa-dvc.org](mailto:membercommunications@amwa-dvc.org) in collaboration  
with



Try email marketing for free today!

---