NAGNF Spotlight
Fall 2021

Are Covid-19 Vaccine Booster Shots Really Required for Everyone?

By Dr. Nana Dadzie Ghansah

As humans, our first line of defense against viral pathogens is the innate immune response. That includes things like the skin, cytokines, and macrophages. This response tries to hold the line till the adaptive immune response system kicks in. This process can take about 7 – 14 days. The adaptive system is made up of the humoral and cellular components. The humoral part has the B-lymphocytes that make antibodies to go after the virus outside the cell. The cellular system is made of T-cells that go after cells that the virus has invaded.

If one survives a viral infection, the body retains a memory of the particular virus in the adaptive system. The antibodies produced to fight the virus hang around, and the T-cells stay primed. It must be noted that there are two types of antibodies – neutralizing and binding antibodies. Neutralizing antibodies play the dominant role in humoral immunity and are the most desired ones. Beyond that, the body also makes memory versions of the B- and T-cells. These come into play in cases where the antibodies decay and as a backup. If there are insufficient levels of neutralizing antibodies when the virus attacks again, the memory T-cells induce the memory B-cells to produce plasma cells. These cells produce antibodies. This process may take about five days. While this attack may result in a measurable infection, it does not usually lead to severe disease or death.

Is SARS-CoV-2 Vaccine Protection Only Dependent on Neutralizing Antibodies?

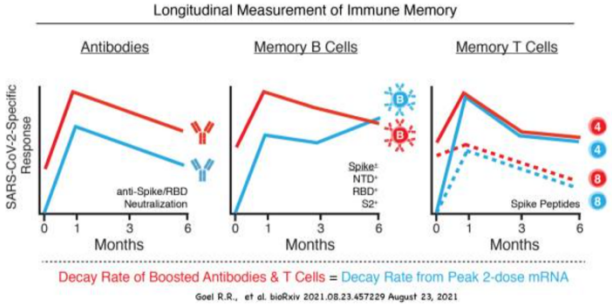
Thus, neutralizing antibodies may decay and show low levels shortly after an infection. Memory cells on the other hand last for decades. If instead of an active infection, one receives a vaccine, a similar process plays out. Where some vaccines lead to antibody levels that last for years, others produce antibodies that decay after months. However, the presence of memory cells offers that same long-lasting protection. With SARS-CoV-2, the virus that causes COVID-19, the neutralizing antibodies seem to decay after about 6-8 months to levels where another infection may not be readily prevented (Sherina N. et al., 2021 , Xiang, T et al. 2021, Crawford, KHD, et al. 2021)[1,2,3].

The decay may be faster in those over 65 years and the immunocompromised. Variants further compound this decay with significant changes in the S-protein. These changes in the antigen used to make the vaccines always raise concerns of drops in vaccine effectiveness. However, in most vaccinated individuals, levels of memory B- and T-cells stay stable or even seem to rise with time. Thus, though there may not be enough neutralizing antibodies available to fight off a new SARS-CoV-2 attack immediately, and a measurable infection by PCR ensues, the memory cells induce the production of active B- and T- cells in a matter of days to fight the new infection. This prevents severe disease and death. Individuals over 65 and the immunocompromised may not survive long enough to benefit from memory cell induced neutralizing antibody production. For these groups of people, keeping high levels of neutralizing antibodies may be advisable. This can be achieved through a booster shot. For most people, however, the booster might not be necessary.

Longitudinal Trends in Neutralizing Antibodies, B and T Memory Cell Decay in Vaccinated Individuals

This study using vaccine naive individuals and previously infected patients may suggest that boosters may not be required for most younger persons with healthy immune systems A group from UPenn looked at this phenomenon in a small study published as a preprint last week. (Goel R.R., Painter, M.M., Apostolidis, S.A., and Mathew, D. et al. bioRxiv 2021.08.23.457229 August 23, 2021)[4].They collected and examined blood samples from 61 individuals, 45 SARS-CoV-2 naïve, and 16 who had recovered

from COVID-19. The study was over six months. From the 45 SARS-CoV-2 naïve individuals, they were able to chart the behavior of the immune response post mRNA vaccine series. Since the group that had recovered from COVID-19 had a similar immune response to those who were vaccinated, they were given a shot of either mRNA vaccine. That allowed the group to study how a booster would work.



Main Take Home Points from The Study

1. Neutralizing antibody levels decayed in all individuals but were still detectable at six months.
2. Functional memory B-cell responses, including those for the receptor-binding domain (RBD) of the alpha, beta, and delta variants, were generated by the mRNA vaccines and continued to increase as of 6 months.
3. Most memory B-cells generated by the mRNA vaccines were capable of cross-binding variants of concern (VOCs).
4. Vaccinated persons produced more memory B-cells that could bind the different variants than those recovering from a mild form of COVID-19.
5. The antigens also boosted cells which are markers of memory T-cell action: CD4+ and CD8+.
6. In the group that got the booster, neutralizing antibody levels increased in the short term but decayed in 3-6 months.
7. The vaccines are doing what they are meant to do; prevent severe disease and death.

Every single data set from hospitals, counties, states, and countries with good vaccination rates show a great dichotomy between hospitalizations for vaccinated and unvaccinated. The vaccines do not impart sterilizing immunity. Thus, vaccinated folks may still harbor the virus even if it is not viable (Shamier, MC et al. medRxiv 2021.08.20.21262158)[5]. Also, the memory cells may not kick in early enough to protect some people, especially those over 65 and the immunocompromised. However, they protect a large group of vaccinees and help reduce the virus' replication and mutation (Niesen MJM et al. medRxiv 2021.07.01.21259833)[6]. Therefore, in the absence of good data it is very likely that more vulnerable individuals, those with impaired immune systems and those older than 65 years may be the ones who really need a booster. So please get the shots, mask up when indoors to protect yourself and the vulnerable ones around you, and above all, stay safe!

By Dr. Nana Dadzie Ghansah, Anesthesiologist, Lexington, Kentucky

1 Sherina, Natalia, et al. "Persistence of SARS-CoV-2-specific B and T cell responses in convalescent COVID-19 patients 6–8 months after the infection." Med 2.3 (2021): 281-295.

2 Xiang, Tiandan, et al. "Declining Levels of Neutralizing Antibodies Against SARS-CoV-2 in Convalescent COVID-19 Patients One Year Post Symptom Onset." Frontiers in Immunology 12 (2021): 2327.

3 Crawford, Katharine HD, et al. "Dynamics of neutralizing antibody titers in the months after severe acute respiratory syndrome coronavirus 2 infection." The Journal of infectious diseases 223.2 (2021): 197-205.

4 Goel, Rishi R., et al. "mRNA Vaccination Induces Durable Immune Memory to SARS-CoV-2 with Continued Evolution to Variants of Concern." bioRxiv (2021).

5 Shamier, Marc C., et al. "Virological characteristics of SARS-CoV-2 vaccine breakthrough infections in health care workers." medRxiv (2021).

6 Niesen, Michiel, et al. "COVID-19 vaccines dampen genomic diversity of SARS-CoV-2: Unvaccinated patients exhibit more antigenic mutational variance." medRxiv (2021).

Deep Lines

By Irene Ahorlu, MSN, CRNA

Looking at her face, there was a weathered look. A look of hard times past - of battles lost and won. A look of triumph and strength but with cares and burdens. I see deep lines...

I see deep lines when she smiles
I see deep lines around her eyes
I see deep lines around her lips
I see deep lines around her nose

But she smiles
A sight to behold
Her smile signifies courage ...
Courage to stare into the jaws of life and say,"Bring it on! You can swallow me up but I'll go down swinging"
"Bring it on! I may not be ready but I'm prepared"

And she dreams
A vision to behold
Her dreams signify hope
Hope in the knowledge that the storms of life are meant to teach her to sail
"Bring it on! You can toss me about but I'm not letting go of the rudder"
"I may not be a sailor but I'm a quick study"

And she speaks
A voice to be heard
Her speech embodies wisdom
Wisdom to understand that the trials of life build an unshakable warrior
"Bring it on! You can throw fiery darts with speed but I'm not retreating"
"Bring it on! I may not be a soldier but I know how to fight"

Then she breathes
A sound to be heard
Her breath signifies restoration
Restoration that brings respite from the tribulations of life.
"Bring it on! You can push me around but I know how to stop and just breathe"
"Bring it on! I may not be a sprinter but I know how to run afar if I just breathe and keep going"

I see deep lines and they tell a beautiful story.

COVID-19 Vaccine Training Modules

https://www2.cdc.gov/vaccines/ed/covid19/index.asp

Could you be a target for cybercrime?

Understanding the potential threats can help keep your online accounts safe.

Courtesy of Fidelity

You've likely spent a good deal of time thinking about investment risk. But have you stopped to think about more personal security issues, such as the safety of your online financial transactions and information stored on your computers? While most people recognize that online fraud or cybercrime is a potential threat, few know how or why they may be at risk. Cybercrime can take many forms, and understanding who the enemies are and how they commit crimes may allow you to better defend yourself.

The "Bad Guy"

Economic cybercriminals pose the greatest online risk to your family's personal financial data and assets. Make no mistake, many of these thieves are highly skilled and sophisticated. They may be individuals or coordinated groups that use technology to steal. For most of us, cybercrime can best be described as an extension of traditional criminal activity focused on personal financial data and monetary theft.

How do cybercriminals operate?

Indiscriminate targeting

In some cases, cybercriminals cast a wide net with "phishing" scams, among others, and hope the sheer quantity of potential victims will yield sufficient economic benefit (see "The makings of a cybercrime," below, for more details on how cybercriminals attack).

Specific victim targeting

A growing and more concerning trend is the specific targeting of high-net-worth individuals. In many of these cases, criminals spend a great deal of time and effort identifying a worthwhile target and then developing a victim profile based on public and private information—such as property records, credit information obtained via hacking, and posted details on social networks—with the goal of stealing assets from financial accounts.

Although the actual criminal act can take several forms, the basic steps are often similar. Below is a relatively common scenario:

Step 1: The thief sends an email with a link or attachment to the victim that appears to come from a known party. The targeted victim then clicks the link or attachment, which includes malicious software (malware) that infects the victim's computer.

Step 2: The thief uses installed malware to steal login credentials to the victim's financial accounts or to remotely control the victim's computer. This will generally allow the thief to log in as the victim.

Step 3: With access to accounts, the thief changes the victim's profile at the financial institution and/or impersonates the victim and moves money to criminal accounts at a different institution.

That's the bad news. The good news is that with some simple steps, you can improve your defenses and reduce your vulnerability to this type of crime.

How do I keep my online accounts safe?

1. Protect your online access with unique user IDs, passwords, and 2-factor authentication for each site

Treat your computers and websites as you would your front door—restrict access and use tough security measures. Passwords are the keys to your online financial information. If cybercriminals find them, they can unlock the doors to your bank accounts, investment accounts, and your personal information. Unfortunately, a significant amount of malicious software trolls the internet looking specifically for account credentials (IDs and passwords). With an inadvertent click on what appears to be a legitimate link or the opening of an attachment designed to look legitimate, this software can be loaded on your machine and be ready to take your "keys."

Go for 2

Adding an additional layer of security when you access your accounts, called 2-factor authentication, is a strong defense against most common attacks. Fidelity and many other financial firms now offer 2-factor authentication. It requires you to enter a unique security code, randomly generated and sent to your phone or other mobile device, in addition to your standard login ID and password. While not completely foolproof, 2-factor authentication raises the bar for cyberattackers trying to access your accounts. Consider enabling 2-factor authentication for nonfinancial sites, such as your mobile phone billing sites (e.g., AT&T, Verizon, T-Mobile, Xfinity) and email sites (e.g., Google Gmail, Apple, Microsoft, Yahoo, Hotmail).

Make sure your financial sites and email providers have your mobile phone number as it is generally used to secure your online access.

Go long and stay strong

You've probably heard this before, but it bears repeating: Never use names, birth dates, Social Security numbers, or any personally identifiable information as your login ID and password. Use a different password for every application and website. Why? The dangers of password reuse. Every year there are data breaches and more sets of credentials (user IDs and passwords) leaked onto the internet. It is common practice these days for criminals to collect these credential dumps and try these login IDs and passwords at financial sites, email providers, mobile phone providers, social media sites, and others. If a Fidelity customer were to use the same password here that they used on another website, and that other account was breached, their Fidelity account could be at risk.

What constitutes a good password? Long (10 or more characters), and complex (combination of special letters and numbers) help make passwords more unique. A string of unrelated words with numbers and special characters in between is best. Stay away from single dictionary words or common combinations of words.

Go with a password manager

These days, most of us have dozens of passwords covering multiple devices and everything from email accounts, telecom billing, and subscription services, to social media, online shopping, and banking. Remembering all these passwords, and changing them frequently, just isn't sustainable and as a result we have a tendency to reuse the same password everywhere. This is the worst practice though. Fortunately, there's an app for that. Password manager apps generate and store all your passwords in a secure environment. They'll even auto-fill login information for stored sites. Many now sync your passwords across all your devices and automatically generate new ones on a regular schedule. The cost of state-of-the-art password managers is negligible—especially when compared with the convenience and security they provide.

2. Secure devices and software, keep them up to date, and perform regular backups

One of the smartest things you can do to keep your financial information safe is to use modern and up-to-date, operating systems. Software makers have teams of cybersecurity specialists dedicated to fixing vulnerabilities in their current systems, and they are always on the lookout for new ways cybercriminals can hack into their products to access users' computer files or install malicious software.

Updating your systems is easier than it used to be

Today, most operating systems let you set your preferences to automatically install updates and patches as soon as they are available. That goes for software too, including antivirus protection. Don't forget to update your mobile phones and tablets, and the apps installed on them. You can set update preferences to do this automatically on your devices.

You can never have too much backup

Backing up your data is good system hygiene. It prevents your information from being lost forever and immunizes you from ransomware attacks. In this increasingly common scheme, criminals lure you into clicking an email link that downloads malware and blocks your access to the computer. The perpetrators can hold your hard drive hostage, demanding a hefty ransom to unblock it. If your system data is backed up elsewhere, it eliminates any leverage the scammers have, neutralizing their threats.

Backups are most effective when done frequently. Savvy users employ redundant methods—typically a USB-connected external storage device in tandem with an encrypted cloud-based service. External

storage offers more immediate data retrieval, while cloud-based services can store much more data. Also, in the event of a flood or fire, both the computer and external storage device may be lost, but offsite backups to a cloud-based service would be safe.

Don't forget to include mobile devices in regular backups. This can be done via a cloud-based service, but a full backup may require connecting to a computer. By syncing up your photos and home movies to your computer, they will then be included in regularly scheduled backups, keeping them secure.

3. Avoid accessing financial accounts or e-commerce sites through links in email

Cybercriminals are getting smarter about making their phishy emails look legitimate. These emails mimic those of financial institutions, complete with logos and convincing signature lines. Sometimes, the criminals impersonate emails appearing to come from friends, family members, or professional contacts you trust. Searching Google and social media sites makes it easy to personalize these emails with your name and subject lines like "Your recent transaction with us." All of this is designed to lower your guard so you'll be more apt to click a link to a fraudulent version of your financial website. This allows the scammers to download malicious software onto your computer or gain access to your passwords and usernames.

When it comes to security, emails cannot be trusted

Avoid clicking links in your emails to access your financial sites online, no matter how compelling the language in the email appears. Instead, go directly to your provider's website by using a link you've saved in your "Favorites" menu. That way, you'll be sure you arrive at a legitimate website. Always look for the "https" prefix in the site's address. This indicates that the connection to the site is encrypted to protect your sensitive data from prying eyes. And if there is an ask by email to send money, always call your contact by phone to confirm the request along with transfer details even if you were expecting the ask.

4. Always access your accounts from a secure Wi-Fi location

Your home Wi-Fi network comes with built-in security. Your network provider supplies you with a wireless router ID and password, but these are default settings. Cybercriminals know the defaults for major network providers. If you're using these settings, your "secure" home Wi-Fi network may not be as secure as you think.

Home networks now connect computers and smartphones to thermostats, TVs, refrigerators, and residential security systems. Each device is a potential weak spot in your Wi-Fi network. As your home becomes more dependent on the internet, so does your exposure to a network breach.

When setting up your home network, consider changing the default WiFi network name and passwords.

Beware of public Wi-Fi

Everyone loves free Wi-Fi, but unsecured public wireless access points are easy to intercept, providing an opportunity for attackers to snoop on your online activity. A safer alternative is to use only secure Wi-Fi networks. If you use your laptop or mobile devices while traveling, purchase a subscription to a paid hotspot provider in which the networks are password protected and have additional levels of security.

5. Consider using a dedicated device for online banking

One of the best ways to secure your online financial information is to dedicate one device exclusively for banking and financial use. Many cyberattacks come from malware installed while you're web surfing and reading emails. Eliminating those activities from a dedicated banking computer goes a long way toward keeping your financial information out of harm's way.

Help us help you

A dedicated banking device also helps financial institutions keep your accounts secure. Most, including Fidelity, monitor client accounts for fraudulent logins from unauthorized computers and will alert you if there is suspicious activity in your account. When Fidelity surveyed client login patterns, we found many users logging in from multiple devices. One or two were common, but some clients routinely logged in from a seemingly random assortment of systems, making it difficult for an institution to distinguish a legitimate login from a fraudulent one. By using one device for all transactions, an illegitimate login stands out, and the institution will be able to move quickly to alert you and secure your account.

6. Understand your computing environment and consider whether you need help

If you have a complex computing environment, a comprehensive cyber-risk assessment may be an appropriate step in protecting your personal information. Individuals with complicated online footprints may want to consider implementing additional systems (e.g., intrusion prevention and detection, firewalls).

Because cyberthreats evolve almost as fast as technology itself, consider retaining a firm to provide ongoing system surveillance, support, and maintenance. These services include everything from monitoring your home internet traffic and blocking outside threats, to educating family members about smart social media practices, safe web surfing and e-commerce protocols.

A good risk assessment will be specific to each person and should consider questions like:

- How many computers, mobile devices, tablets, TVs, home security systems, and appliances are connected to your home Wi-Fi network?
- Are they shared across personal and business or home office use?
- Do non-family members regularly in your home have access to your Wi-Fi network or computing devices?
- What backup procedures are in place for each device?
- Are you or other household members active on social media like Facebook, Twitter, or Pinterest?

Conclusion

No one wants to spend time thinking about all the bad things that can happen, but it's important to understand potential threats to your assets and take measures to eliminate them. When it comes to protecting your financial accounts from cyberthreats, practicing good system hygiene and making a few changes in your online habits will significantly improve your security. You play a key role in helping Fidelity detect fraud by maintaining a general awareness of your accounts, including staying alert to notifications regarding password resets, money transfers and account changes, and periodically logging in and checking for unusual transactions and activity.

Fidelity uses sophisticated security measures to protect our customers. We also make many additional security tools available for customers to utilize, including 2-factor authentication and transaction alerts. Of course, we also provide a Customer Protection Guarantee for fraudulent activity. Make sure to visit Fidelity's online customer security site to explore some of these features, and learn more about what Fidelity is doing to help keep your assets safe.

Please, we need your input!

Are you a Ghanaian who has cared for loved ones in the USA with a stroke?

Are you a Ghanaian who is a survivor from a stroke?

Do you know a Ghanaian who survived a stroke?

Please share your experience with us.

Please reach out to me at 914 266 0803.

You will receive a gift card and a regulated thermal bag for your appreciation.

Thank you,

Angela Adjetey Appiah
DNP, MPH, RN, COA, FAACM

Executive Corner

Collaborating to promote health

It has been a tough year collaborating to do anything. For a young organization like ours with a mission to be part of the healthcare solutions in our beloved country, it has been a journey requiring realignment and readjustments at several levels. This new era of COVID-19 presents several challenges to both personal and professional relationships across several platforms. However, the challenges have also pushed us to dig deep and derive ways to mitigate these challenges. One very notable mitigating process is the discovery of Zoom and the other online platforms that provide real time platforms to meet even across continents. In fact, these online platforms have been so effective that it's being used across several organizations to a point where terms like "COVID fatigue" are becoming a reality.

Our organization is not exempt from the dynamics of the online meeting platforms. Zoom has been of tremendous advantage to our collaborative agenda. In November 2020, we had our first annual conference on Zoom, which brought several of our members across the nation and international partners together for a very successful educational session. We also conduct all our board meetings on Zoom. Several of our members are part of joint education agendas on Zoom platforms. A notable example is the joint YALE/NAGNF/Korle-Bu Critical-Care nurse education agenda and the joint international nurses' platform formed to assist in separating conjoined twins, a groundbreaking procedure in Ghana.

Collaborating to promote health is truly what it is all about. Being part of a diverse group of professionals, sharing information and presenting professional opinions for discussion across that platform by like-minded individuals is what drives solutions. So yes COVID brought several obstacles and road blocks, but with sheer determination to meet our goals we dig deep and continue to create new pathways to continue with our mission. We continue to take every opportunity to collaborate to promote health at no matter what. Let us join hands together and continue on that path.

Gifty Lano, RN
NAGNF President

NAGNF Spotlight

Fall 2021 Contributors:
Cheryl Maafoh
Irene Ahorlu
Gify Lano
Nana Dadzie Ghansah

Tel: +1 570 422 1095
Email: info@nagnf.org
Website: https://nagnf.org/
Facebook: https://www.facebook.com/NAGNF1/