

VA took swift action to disconnect from all affected systems and protect Veterans

Editor's note: This post was updated 7/26/2024 to inform readers of the upcoming July 29 mailings.

You may have heard in the news about the recent Change Healthcare (CHC) [cybersecurity incident](#), which impacted many health care institutions across America. We at VA want to provide an update on what this incident could mean for you.

CHC is one of VA's vendors, and as soon we became aware of the breach we took swift action to disconnect from all known systems with CHC; we have confirmed that there is no malicious activity or irregularities in our system.

However, CHC [announced this week](#) that "a substantial portion of the people in America" could have had some protected health information leaked as a result of this incident. While there is no confirmation that Veteran data was leaked as a result of this incident, we want to provide you with all of the information that you could need to protect yourself.

Here's what you need to know:

- CHC is notifying impacted individuals via U.S. mail beginning July 29. The letters explain how you may have been impacted and steps you can take to protect your identity online.
- CHC is offering credit monitoring for all impacted individuals. CHC will provide two years of free credit monitoring and identity theft protections for those impacted. You can call 1-866-262-5342 or visit [the dedicated UHG/CHC website](#) at <http://changeybersupport.com> to learn more.
- VA has general fraud protection information available to you. There are always steps that you can take to protect yourself against fraud and identity theft, and VA has resources available to you. General information on how to protect yourself from fraud is available at [Protecting Veterans From Fraud | Veterans Affairs \(va.gov\)](#). This includes a [fraud protection toolkit](#), frequently asked questions, information about how to be vigilant about scams, and much more.
- The federal trade commission also offers resources to help protect your identity. For additional information about other precautions available to you, visit [the Federal Trade Commission website](#) at <http://www.consumer.ftc.gov/features/feature-0014-identity-theft>.
- VA health care operations are not impacted. While we work through this issue, we want you to know that VA remains fully open for business—and there is no known adverse impact on VA patient care or outcomes to date. Please do not hesitate to come to us for all of your health care needs, as usual.

At this time, we cannot confirm that any Veteran data has been compromised, so we cannot answer specific questions as to whether your data is involved. But if it is determined that Veteran

data was included in the data breach, we will ensure that you are notified and full support is provided.

Protecting your personal health information is—and always will be—one of our top priorities. We will continue to monitor this incident closely and provide updates whenever possible.

[Link Disclaimer](#)

This page includes links to other websites outside our control and jurisdiction. VA is not responsible for the privacy practices or the content of non-VA Web sites. We encourage you to review the privacy policy or terms and conditions of those sites to fully understand what information is collected and how it is used.

**“Be on your guard, stand firm in the faith, being men of courage, be strong.”
1Cor 16:13**

Sincerely,

William A. Harris, Jr.

William A. Harris, Jr.

William A. Harris, Jr., USAF Retired

President, Veterans for Christ, Inc.

www.veteransforchristinc.org

Need to contact VA?

[Veterans Crisis Line: 1-800-273-8255](#) and press 1, [Chat](#), or Text 838255

[Homeless Veteran Resources: 1-877-424-3838](#) or [Chat](#)

[White House VA Hotline: 1-855-948-2311](#)

[1-800-MyVA411 \(800-698-2411\)](#) is never the wrong number