VERMONT
DEPARTMENT OF HEALTH

Health Alert
October 31, 2020

TO: Vermont Healthcare Partners

FROM: Vermont Department of Health

Increased and Imminent Cybercrime Threat

The Department of Health and Human Services (HHS), the Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Bureau of Investigation (FBI) have credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers. The Vermont Department of Health is sharing this warning so that providers may take timely and reasonable precautions to protect their networks.

CISA has posted a joint cybersecurity advisory that describes the threat and the tactics, techniques, and procedures used by cybercriminals against targets in the Healthcare and Public Health Sector, often leading to ransomware attacks, data theft, and the disruption of healthcare services. **View the full advisory with threat details and best practices here**: https://us-cert.cisa.gov/ncas/alerts/aa20-302a

The Vermont Department of Health encourages healthcare providers to take immediate action in protecting their Information Systems and to consider following the advisory's mitigation steps.

Additionally, the Department of Public Safety strongly recommends that all users be mindful of these essential security tips to protect your facility and personal accounts. Here are 10 of the top security tips:

1. Recognize that every user is a target.
2. Practice good password management. Use a variety of characters. Avoid using the same password for different accounts. Don't write passwords down, especially near your computer.
3. Ensure your computer and external devices remain attended or locked.
4. **Be VERY careful when clicking on attachments or links in email**. If it's unexpected or suspicious for any reason, don't click on it. Double check the address of the website the link is pointing to: look for spelling mistakes or addresses similar to but different than real addresses.
5. Banking or work-related browsing that involves secure information should only be done on a device that belongs to you and on a trusted network (e.g. not public computers and public WiFi).
6. Back up data regularly.
7. Be sure your anti-virus software is always up to date.
8. Be cautious of what you plug in to your computer.
9. Be mindful of what you share publicly (e.g. on social media). Information posted there can be used to accelerate vulnerabilities.
10. Monitor your accounts for any suspicious activity. Contact your vendor if you see anything unusual immediately.

If you see any suspicious activity, report it immediately to a supervisor and IT team.

And if you see something, say something.
To report related suspicious or criminal activity, contact Vermont Emergency Management at 1-800-347-0488 or the FBI's 24/7 Cyber Watch at 855-292-3937 (or by email at CyWatch@fbi.gov.)

Please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.

Contacting the U.S. Food and Drug Administration:

In general , if you think you had a problem with your medical device or a medical device your patient uses, the FDA encourages you to report the problem through the MedWatch Voluntary Reporting Form.

For urgent matters, such as potential medical device impacts related to a cyber attack affecting your hospital system, please contact CyberMed@fda.hhs.gov.

HAN Message Type Definitions
Health Alert: Conveys the highest level of importance; warrants immediate action or attention.
Health Advisory: Provides important information for a specific incident or situation may not require immediate action.
Health Update: Provides updated information regarding an incident or situation; unlikely to require immediate action.
Info Service Message: Provides general correspondence from VDH, which is not necessarily considered to be of an emergent nature.