Cyber Security Practices during COVID-19

While governments and healthcare systems around the world are striving to keep patients and providers safe from COVID-19, they must also be careful to keep their guard against cyber predators seeking to exploit the panic. The risk has grown so much that Interpol released a Purple Alert in April 2020[1] warning organizations globally that cyber criminals have begun targeting critical healthcare institutions with ransomware.

With staff and organizations scrambling to support patients it is easy to overlook basic practices used to secure business information, allowing cyber criminals to penetrate systems. Furthermore, employees trying to do the 'right thing' for distressed patients might let down their guard. The result could be malicious viruses called 'ransomware' embedded in emails or installed on systems locking data and access until a payment is made, usually through an untraceable mechanism such as Bitcoins.

Emboldened criminals contact organizations by email or phone claiming to be from government agencies and requesting access to data or asking an email recipient to click on an attachment which will install the ransomware.[2] INTERPOL is providing technical support and advice to help protect healthcare systems. This includes collecting and analyzing suspect Internet domains related to COVID-19, and then taking action with the authorities in those countries.

This is all in addition to the growing threat to patient privacy and care as well as businesses. In 2019 more than 35 million medical records and radiology studies were exposed, with 426 separate breaches and 759 ransomware attacks reported in the US alone, making healthcare one of the most prominent targets for criminals.[3]

We recommend that you follow your institution's IT and Cybersecurity governance practices to help keep your patients and healthcare systems secure. Human error remains the major source of such cybersecurity breaches in most cases, and healthcare is not immune.[4] The best way to safeguard your organization is to have official Cyber Security Policies and Procedures with ongoing monitoring and education to ensure they are for understood and followed.

If you do not have established Cyber Security guidelines for your organization, please contact your IT and Equipment providers for recommendations.

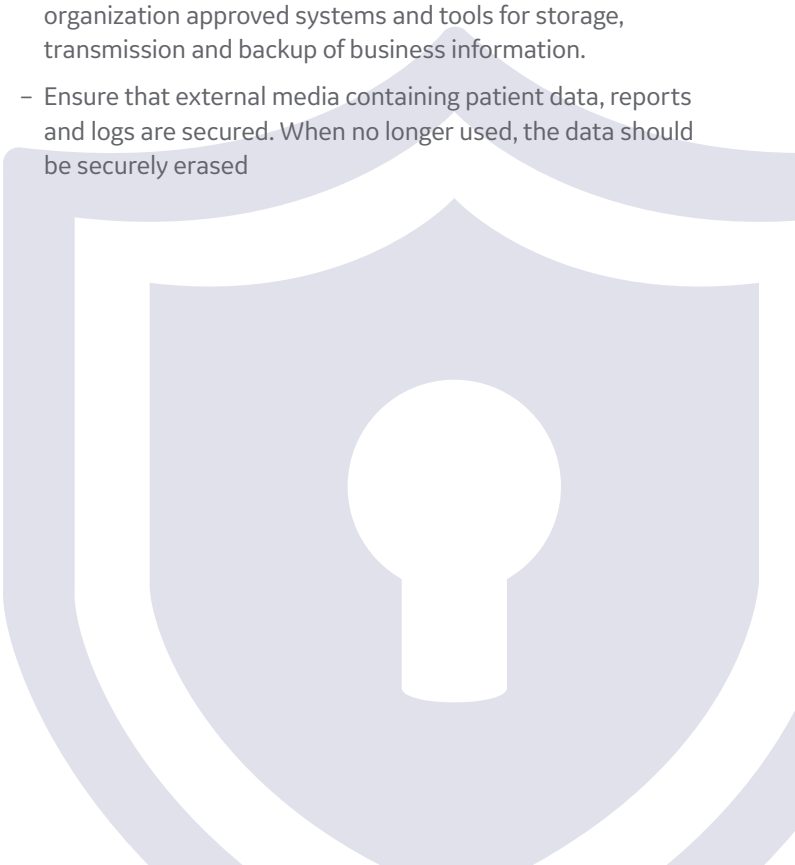
What the experts recommend

Interpol recommends several steps hospitals and healthcare organizations can take to protect their systems and IT infrastructure. These include:

- Only opening emails or download software/applications from trusted sources;
- Not clicking on links or open attachments in emails which you were not expecting to receive, or come from an unknown sender;
- Securing email systems to protect from spam which could be infected;
- Backing up all important files frequently, and store them independently from your system (e.g. in the cloud, on an external drive);
- Ensuring that software which detects the presence of malware (e.g. anti-virus, application whitelisting) is installed and enabled on all applicable systems and mobile devices;
- Using strong, unique passwords for all systems, and updating them regularly

Other guidelines to consider in your organization include:

- Awareness of Cyber Criminal practices:
  - Know the common signs and carriers of phishing (e.g. phone calls, emails, SMS, social media) and recognize efforts to improperly acquire organization information
  - Do not use permit use of personal email, unapproved devices and software to conduct organization business
  - When posting information online, avoid the disclosure of personal information, proprietary or other sensitive information
- Prevent unauthorized access, accidental loss, disclosure or destruction of your patient and business sensitive information:
  - Secure physical copies and storage areas, as well as areas around computers and equipment with data
  - Encourage staff and operators to lock computers and equipment after use. Implement automatic system locking after a period of inactivity
- Keep your IT networks secure
  - Ensure that all available network security measures and best practices are adopted and that your medical devices are operated in secure network environments that is protected from unauthorized intrusion. There are many effective techniques for isolating and protecting medical information systems, including implementing firewall protection and Virtual Local Area Networks (VLANs)
  - Maintain a list of authorized operators to control access to your devices, enable user authentication and set customized users and passwords
  - Ensure to keep your systems up to date by installing the latest security updates available
  - Do not allow the use of shared accounts and passwords
- Secure your Data storage devices
  - Avoid USB sticks for data storage where possible. Use only organization approved systems and tools for storage, transmission and backup of business information.
  - Ensure that external media containing patient data, reports and logs are secured. When no longer used, the data should be securely erased



Taking steps to secure your equipment

Your Voluson™ systems from GE Healthcare rely on the latest and most advanced security features with the flexibility needed to efficiently manage your practice while ensuring to meet the above guidelines.

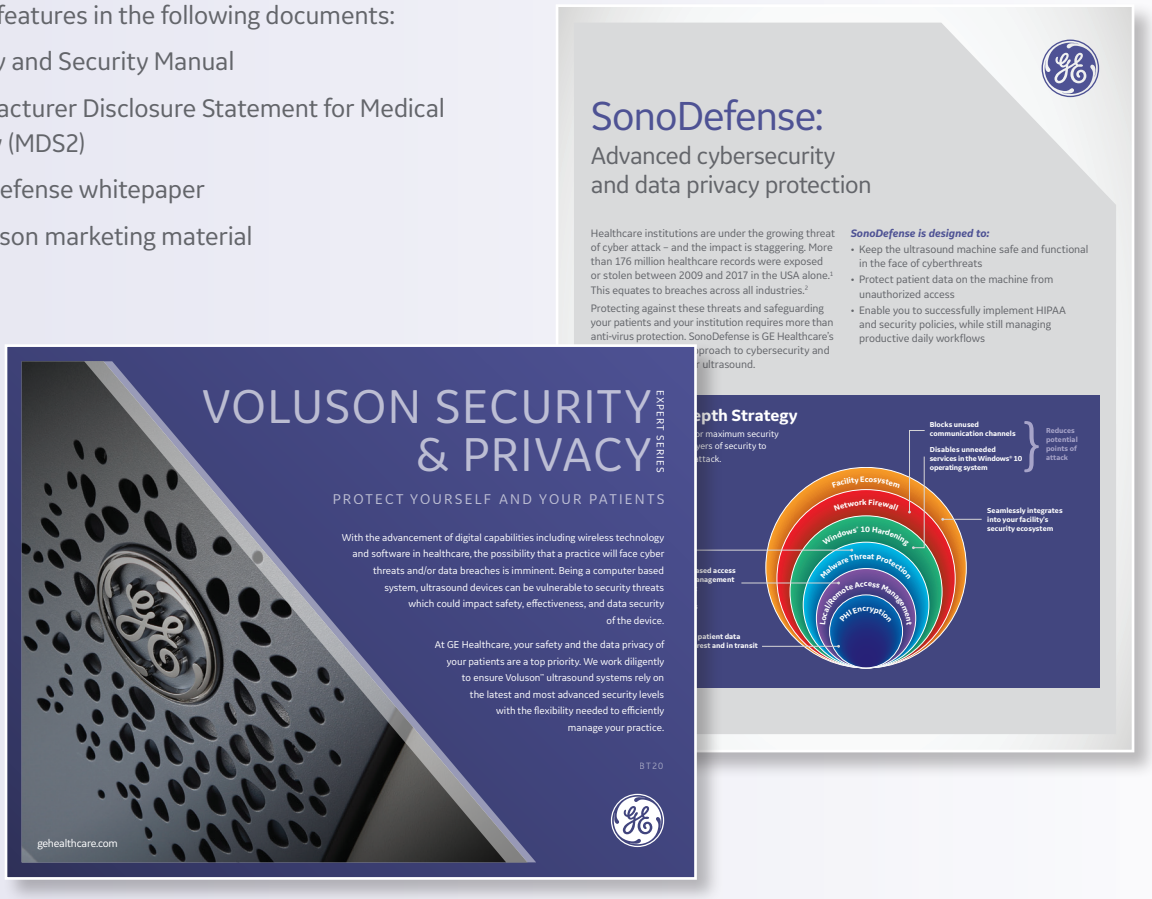
Become familiar with such security features and secure use practices by reviewing available documentation including security disclosure forms and security user manuals. Ensure that you understand the potential risks associated with a security incident and the relative types of risks, some of which may be more critical to patient care, others more relevant to data protection. As your sales or service representatives if you have any questions.

Compared to general purpose IT equipment like laptops, your Voluson systems are special purpose devices which can be used only for their intended clinical purposes. This property allows GE Healthcare to integrate a set of preventive security measures and mechanisms in Voluson systems which drastically reduce the exposure to malware including (but not limited to):

- Disabling features and services (like email reception, internet browsing, etc.) which are commonly used as malware carriers
- Blocking the execution of any computer program and application (including malware) that is not contained in a “whitelist” of programs and applications that are authorized by GE Healthcare to be present or active on the Voluson system

You can find the entire list of system security hardening measures supported and a detailed description of all the Voluson security features in the following documents:

- Voluson Privacy and Security Manual
- Voluson Manufacturer Disclosure Statement for Medical Device Security (MDS2)
- Voluson SonoDefense whitepaper
- Additional Voluson marketing material



References

1. Interpol – Cybercriminals targeting critical healthcare institutions with ransomware, April 4, 2020.

   https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware

2. Forbes: Healthcare Workers Targeted By Dangerous New Windows Ransomware Campaign Using Coronavirus As Bait, Mar 22, 2020.

   https://www.forbes.com/sites/daveywinder/2020/03/22/healthcare-workers-targeted-by-dangerous-new-windows-ransomware-campaign-using-coronavirus-as-bait/#537fe5e72212

3. Cyber MDX 2020 Vision: A Review of Major IT & Cybersecurity Issues Affecting Healthcare, Mar 2020.

   https://www.cybermdx.com/resources/2020-vision-review-major-healthcare-it-cybersec-issues

4. 24x7 COVID-19 Pandemic Exposes Healthcare Facilities to Cybercriminals, Apr 26, 2020.

   https://www.24x7mag.com/standards/safety/cybersecurity/cybercriminals-targeting-critical-healthcare-institutions-covid-19-pandemic/

June 2020
JBXXXXXX