May 15, 2017

The United States Computer Emergency Readiness Team (US-CERT) has received multiple reports of ‘WannaCry’ (also known as ‘WannaCrypt’) ransomware infections in several countries around the world and in the United States.  Some of these infections are impacting patient access to care.  [Ransomware](https://urldefense.proofpoint.com/v2/url?u=http-3A__links.govdelivery.com-3A80_track-3Ftype-3Dclick-26enid-3DZWFzPTEmbWFpbGluZ2lkPTIwMTcwNTEzLjczMzI4MzkxJm1lc3NhZ2VpZD1NREItUFJELUJVTC0yMDE3MDUxMy43MzMyODM5MSZkYXRhYmFzZWlkPTEwMDEmc2VyaWFsPTE3NDE0OTE5JmVtYWlsaWQ9bGF1cmEuaG9mZm1hbkBhbWEtYXNzbi5vcmcmdXNlcmlkPWxhdXJhLmhvZmZtYW5AYW1hLWFzc24ub3JnJmZsPSZleHRyYT1NdWx0aXZhcmlhdGVJZD0mJiY-3D-26-26-26101-26-26-26https-3A__www.us-2Dcert.gov_security-2Dpublications_Ransomware&d=DwMFAA&c=iqeSLYkBTKTEV8nJYtdW_A&r=mcnYQDCWr4rQPlqPQfKcKBlbQUCoVMQcoKHheNR0vZg&m=PmzAD0IOdUg9aPJMiJMjP75DpZ3UzAfnj1IQ2YIDsk4&s=MYyvOgyZx_UM_pQV7blymsz0KVat7H1zzbtsXJ6w46o&e=) is a type of malicious software that infects a computer and restricts users’ access to it until a ransom is paid to unlock it.  Individuals and organizations are discouraged from paying the ransom, as this does not guarantee access will be restored.

In addition to the information provided below, the AMA has resources to help physicians [conduct a checkup](https://www.ama-assn.org/delivering-care/how-improve-your-cybersecurity-practices) of their systems, and to [secure their networks](https://www.ama-assn.org/delivering-care/network-security) and [office computers](https://www.ama-assn.org/delivering-care/checklist-office-computers).  Additionally, the AMA has been engaged with the administration since the cyberattack and will continue to monitor the situation to update you as more information becomes available.  In the meantime, please let us know by replying to this email whether your members have been impacted by the WannaCry infection.

**What Should I Do Now?**

Ransomware can infect computers and medical devices.  The WannaCry infection affects systems running Windows and spreads easily when it encounters unpatched or outdated software.  **Physicians should ensure that their computer’s operating systems and anti-virus software are updated and patched:**

* Run Windows Update immediately.  Download and install any available updates (‘patches’).  Run a scan on your anti-virus software and follow its prompts.  Microsoft has released a customized [patch](https://urldefense.proofpoint.com/v2/url?u=https-3A__blogs.technet.microsoft.com_msrc_2017_05_12_customer-2Dguidance-2Dfor-2Dwannacrypt-2Dattacks_&d=DwMFAg&c=iqeSLYkBTKTEV8nJYtdW_A&r=xco41HArmWqJXtFVtePW2d7cATLhXcl1eeKY6ePIx6g&m=jKzfLEF86nkodteXuLbMB_6QkVrlTLofyBBsxzIenZU&s=5Lf9bkvedGQdvY2Y-_9xH6eT0XnvUS2J1PhdoMyQljY&e=) for older platforms that do not receive mainstream updates, including Windows XP, Windows 8, and Windows Server 2003. At this time, Windows 10 has not been targeted by the attack.
* Check your computer’s settings to ensure that the system will automatically download and install new versions of the operating system and Microsoft Office software.  Do the same for your anti-virus software.
* Note when the computer will install these new updates and make sure the computer is on at that time.

**In addition, physicians should contact their medical device vendors and manufacturers to ensure that they have patched their device software**.  Medical device manufacturers can always update a medical device for cybersecurity; the FDA does not typically need to review changes made to medical devices solely to strengthen cybersecurity.

**How to Help Protect Yourself from Downloads and Email-Based Ransomware**

Ransomware can be delivered via email by attachments or links within the email.  Attachments in emails can include documents, zip files, and executable applications.  Malicious links in emails can link directly to a malicious website the attacker uses to place malware on a system.  To help protect yourself, be aware of the following:

* **Only open emails from people you know and that you are expecting.** The attacker can impersonate the sender, or the computer belonging to someone you know may be infected without his or her knowledge.
* **Do not open email attachments from an unknown, suspicious, or untrustworthy source.**  If you're not familiar with the sender, do not open, download, or execute any files or email attachments.
* **Do not open an email attachment unless you know what it is, even if it appears to come from a friend or someone you know.**  Some viruses replicate themselves and spread via email.  Stay on the safe side and confirm that the attachment was sent from a trusted source before you open it.
* **Do not open any email attachments if the subject line is questionable.**  If you think that the attachment may be important to you, always save the file to your hard drive before you open it.
* **Vigilance is the best defense against phishing scams.**  “Phishing” describes email scams that attempt to acquire confidential information such as credit card numbers, personal identity data, and passwords.  Often these emails look like they come from real companies or trusted individuals.  If you want to find out whether the email is legitimate, contact the company via their published customer service contacts.  Do not reply to the email or click on any links.
* **Exercise caution when downloading files from the internet.**  Make sure that the website is legitimate and reputable.  If you have any doubts, don't download the file.
* **Do not open messages or click on links from unknown users in your instant messaging program.** Instant messaging can be a vehicle for transmitting viruses and other malicious code, and it’s another means of initiating phishing scams.

**Example of Ransomware**

This is an example of what the ransomware may look like:



**What to Do If You Have Been Infected**

If your organization is the victim of a ransomware attack, contact law enforcement immediately.

1. Contact your FBI Field Office Cyber Task Force immediately to report a ransomware event and request assistance. These professionals work with state and local law enforcement and other federal and international partners to pursue cyber criminals globally and to assist victims of cyber-crime.
2. Report cyber incidents to the US-CERT and FBI's Internet Crime Complaint Center.
3. For further analysis and healthcare-specific indicator sharing, please also share these indicators with HHS’ Healthcare Cybersecurity and Communications Integration Center (HCCIC) at HCCIC\_RM@hhs.gov.

**Additional Resources**

* The U.S. Computer Emergency Readiness Team – [US-CERT.gov](https://urldefense.proofpoint.com/v2/url?u=https-3A__www.us-2Dcert.gov_&d=DwMFAg&c=iqeSLYkBTKTEV8nJYtdW_A&r=xco41HArmWqJXtFVtePW2d7cATLhXcl1eeKY6ePIx6g&m=jKzfLEF86nkodteXuLbMB_6QkVrlTLofyBBsxzIenZU&s=OqbS9a6jz-56-JJlTvrfxqrS3KQNVsRAn_1OwWELbXo&e=)
* HHS Office of Civil Rights [Guidance on HIPAA and Ransomware](https://urldefense.proofpoint.com/v2/url?u=https-3A__www.hhs.gov_sites_default_files_RansomwareFactSheet.pdf&d=DwMFAg&c=iqeSLYkBTKTEV8nJYtdW_A&r=xco41HArmWqJXtFVtePW2d7cATLhXcl1eeKY6ePIx6g&m=jKzfLEF86nkodteXuLbMB_6QkVrlTLofyBBsxzIenZU&s=slcsdF7uvDjHtgO89oat--QlcSS58lxVfLb2wD9FC1s&e=)
* [The FDA’s Role in Medical Device Cybersecurity](https://urldefense.proofpoint.com/v2/url?u=https-3A__www.fda.gov_downloads_MedicalDevices_DigitalHealth_UCM544684.pdf&d=DwMFAg&c=iqeSLYkBTKTEV8nJYtdW_A&r=xco41HArmWqJXtFVtePW2d7cATLhXcl1eeKY6ePIx6g&m=jKzfLEF86nkodteXuLbMB_6QkVrlTLofyBBsxzIenZU&s=U2MOFduOWrpHTdYAI6IF5DdfQnh7j8UE4OmE5au4Vp4&e=)
* HHS ASPR - Technical Resources, Assistance Center, and Information Exchange (TRACIE) [Healthcare Emergency Preparedness Information Gateway](https://urldefense.proofpoint.com/v2/url?u=https-3A__asprtracie.hhs.gov_&d=DwMFAg&c=iqeSLYkBTKTEV8nJYtdW_A&r=xco41HArmWqJXtFVtePW2d7cATLhXcl1eeKY6ePIx6g&m=jKzfLEF86nkodteXuLbMB_6QkVrlTLofyBBsxzIenZU&s=RsAUXQh1rSeJt6tUnWX4NJW26HLrtrIi9hszE8Dsh4s&e=)’s [cybersecurity resources](https://urldefense.proofpoint.com/v2/url?u=https-3A__asprtracie.hhs.gov_technical-2Dresources_86_Cybersecurity_86&d=DwMFAg&c=iqeSLYkBTKTEV8nJYtdW_A&r=xco41HArmWqJXtFVtePW2d7cATLhXcl1eeKY6ePIx6g&m=jKzfLEF86nkodteXuLbMB_6QkVrlTLofyBBsxzIenZU&s=ybGVqzOCcietm3CdFNnp8FjKs_f1sYaIhPJ6pAGking&e=)
* The Office of the National Coordinator for Health Information Technology’s (ONC) [SAFER Guides](https://assets.ama-assn.org/sub/advocacy-update/2017-04-20.html), which include [ransomware prevention and mitigation strategies](https://urldefense.proofpoint.com/v2/url?u=https-3A__www.healthit.gov_safer_sites_safer_files_guides_safer-5Fcontingency-5Fplanning.pdf&d=DwMFAg&c=iqeSLYkBTKTEV8nJYtdW_A&r=xco41HArmWqJXtFVtePW2d7cATLhXcl1eeKY6ePIx6g&m=jKzfLEF86nkodteXuLbMB_6QkVrlTLofyBBsxzIenZU&s=PprfZG80aiwoc111jm5_V5eDTLCqgiXuVXimKMw8yLk&e=) (for more information, see the AMA’s recent [Advocacy Update](https://assets.ama-assn.org/sub/advocacy-update/2017-04-20.html))