Report on Patient Privacy Volume 22, Number 2. February 10, 2022 Privacy Briefs: February 2022

By Jane Anderson

◆ **Tensions between the U.S. and Russia could lead to a heightened risk of Russian state-sponsored cyberattacks on U.S. interests, including health care organizations, federal agencies warned.** Russia would consider conducting a cyberattack on the U.S. homeland if Moscow perceived that a U.S. or NATO response to a potential Russian invasion of Ukraine threatened Russia's long-term national security, according to a Department of Homeland Security intelligence bulletin obtained by CNN.[1] 1 The Cybersecurity & Infrastructure Security Agency (CISA), FBI and the National Security Agency have urged organizations to be prepared with cyber incident response, resilience, and continuity of operations plans so that critical functions and operations can be kept running if technology systems are disrupted or need to be taken offline. The three agencies also urged organizations to enhance their cyber posture by following best practices, and to increase organizational vigilance by staying current on threat reporting.[2] John Riggi, national advisor for cybersecurity and risk at the American Hospital Association, warned that hospitals and health systems could be targeted directly, or could become "incidental victims or collateral damage of Russian-deployed malware or destructive ransomware that inadvertently penetrates U.S. health care." Riggi noted that "a cyberattack could disrupt a mission-critical service provider to hospitals," and added that "this is a good reminder for all to have robust downtime procedures, redundancy and business continuity plans to sustain a loss of on-premises or cloud-based mission-critical services or technology for up to four to six weeks."[3]

◆ **CISA also advised U.S. critical infrastructure organizations to review a Microsoft blog on malware identified in Ukraine and take action to strengthen their networks against potential cyberattacks.**[4] The Microsoft Threat Intelligence Center reported evidence of destructive malware in systems belonging to several Ukrainian government agencies and organizations that work closely with the Ukrainian government.[5] The malware is disguised as ransomware, but if activated by the attacker, it would render the infected computer system inoperable. "As we have seen in the past, destructive malware targeting Ukraine can spread rapidly across the globe," said Riggi. "It is again strongly recommended to assess any direct, 3rd party business associate connections and email contacts in Ukraine and that region of the world. Consider blocking such connections. Although geo-fencing for all inbound and outbound traffic related to Ukraine and that region may help mitigate direct cyber risk presented by this threat, it will have limited impact in reducing indirect risk, in which the malware transits through other nations, proxies and third parties. Thus, increased monitoring of networks and incident response preparedness is also strongly recommended."[6]