Attachment R: 2018 NAMCS FAQs

NAMCS FAQs

WHO WILL SEE MY ANSWERS?

We take your privacy very seriously. All information that relates to or describes identifiable characteristics of individuals, a practice, or an establishment will be used only for statistical purposes. NCHS staff, contractors, and agents will not disclose or release responses in identifiable form without the consent of the individual or establishment in accordance with section 308(d) of the Public Health Service Act (42 U.S.C. 242m(d)) and the Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA, Title 5 of Public Law 107-347). In accordance with CIPSEA, every NCHS employee, contractor, and agent has taken an oath and is subject to a jail term of up to five years, a fine of up to $250,000, or both if he or she willfully discloses ANY identifiable information about you. In addition, NCHS complies with the Federal Cybersecurity Enhancement Act of 2015 (6 U.S.C. §§ 151 & 151 note). This law requires the federal government to protect federal computer networks by using computer security programs to identify cybersecurity risks like hacking, internet attacks, and other security weaknesses. If information sent through government networks triggers a cyber threat indicator, the information may be intercepted and reviewed for cyber threats by computer network experts working for, or on behalf of, the government.

WHAT DO MY ANSWERS HAVE TO DO WITH CYBERSECURITY?

The Federal Cybersecurity Enhancement Act of 2015 allows software programs to scan information that is sent, stored on, or processed by government networks in order to protect the networks from hacking, denial of service attacks, and other security threats. If any information is suspicious, it may be reviewed for specific threats by computer network experts working for the government (or contractors or agents who have governmental authority to do so). Only information directly related to government network security is monitored. The Act further specifies that such information may only be used for the purpose of protecting information and information systems from cybersecurity risks.

WHAT DOES "MONITOR" MEAN IN THE ADVANCE LETTER?

"Monitor" means "to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system"; "information system" means "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information"; "cyber threat indicator" means "information that is necessary to describe or identify security vulnerabilities of an information system, enable the exploitation of a security vulnerability, or unauthorized remote access or use of an information system."