Deletions

Due to changes in the confidentiality language, all references to the Federal Cybersecurity Enhancement Act of 2015 in the Assurance of Confidentiality will be deleted. **Please see the deletions below**.

NOTICE - Public reporting burden of this collection of information is estimated to average 30 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to: CDC/ATSDR Information Collection Review Office; 1600 Clifton Road, MS D-74, Atlanta, GA 30333, ATTN: PRA (0920-1015).
Assurance of Confidentiality - 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.~~

~~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.~~

Changes made to reduce burden and improve data collection

We have replaced the term “mid-level provider” with “advanced practice provider” in Question 9 in accordance with the Department of Health and Human Services definition given in 84 FR 7714 and in response to a comment. Questions 23 and 24 were switched so that the questions about the template-based note use in electronic health records (EHRs) are not asked of physicians who do not have EHRs. This will reduce burden for physicians without EHRs. As a result, the skip pattern instructions were updated in Question 19. A ‘not-applicable’ response option was added to questions 26, 36, and 37a to allow physicians to whom these questions do not apply to have an appropriate response. Lastly, wording was changed slightly in Question 44 so that all responses could fit on one line. The “Greater than 2 hours to 4 hours” response was changed to “More than 2 hours to 4 hours.” No additional changes to content were made for the proposed 2020 NEHRS questionnaire.