Electronic Healthcare Network Accreditation Commission

www.EHNAC.org

Lee B. Barrett
Executive Director

Debra C. Hopkinson
Operations, VP
Dhopkinson@ehnac.org

January 23, 2019

Office of Security and Strategic Information (OSSI)
200 Independence Ave, SW
Washington, DC 20201

RE: RFI Section 4002 "*Strategy on Reducing Regulatory and Administrative Burden Relating to the Use of Health IT and EHRs"*

To Whom It May Concern:

The Electronic Healthcare Network Accreditation Commission (EHNAC) appreciates the opportunity to comment on this draft for public comment entitled "Strategy on Reducing Regulatory and Administrative Burden Relating to the Use of Health IT and EHRs" document.

Founded in 1993, the Electronic Healthcare Network Accreditation Commission (EHNAC) is an independent, federally recognized, standards development organization and tax-exempt 501(c) (6) non-profit accrediting body designed to improve transactional quality, operational efficiency and data security in healthcare. EHNAC's accreditation programs are specifically designed to support the protection of electronic health information with a focus on Protected Health Information (PHI) and Personally Identifiable Information (PII) as well as support for industry-adopted standards allowing for a more seamless information exchange between participants in health information networks. EHNAC has over 18 stakeholder-specific programs available across the industry including by not limited to Health Information Exchanges (HIE's), Health Information Service Providers (HISPs), Electronic Healthcare Networks (EHN's), Electronic Prescription of Controlled Substances (EPCS). This includes new programs under development such as one for the use of Blockchain technologies and Trusted Exchange components as set forth within the 21st Century Cures proposed TEFCA requirements.

EHNAC supports the aim of burden reduction, especially for providers. However, burden reduction must not interfere with the primary aim of the EHR – the recording of patient medical information. As well, the accuracy, safety, and security of patient information must be protected. Our comments reflect these two overall considerations.

The title of the document refers to reducing burden in the use of Health IT and EHRs, but the recommendations are a mix of policy (e.g. reducing documentation burdens, aligning reporting requirements across programs) and IT recommendations (e.g. improving presentation, improving functionality). Many of the policy

recommendations relate to reducing burden whether or not HIT is used. We believe that overall burden reduction in program requirements (public health reporting, grant funding, documentation) is a worthwhile goal, but needs to be separate from a paper on reducing burden of Health IT.

The report recommends a variety of changes and standardization to EHRs. We would recommend that costs of changes and upgrades be considered in any recommendation. Providers have indicated that there is a large cost in EHR implementation and upgrades, so that burden must be considered in recommending changes to technology. Cost benefit analyses, especially for providers, should be conducted on many of these recommendations before they are finalized. Standard functionality has proven to be a step in the right direction in that because all products are required to meet the same function, the cost of technical changes can be somewhat spread across the vendors and providers alike, thus possibly alleviating some of the burden on the provider.

Specific comments on the document are:

P 32 – it is noted that the CCD may contain "too much information". EHNAC believes that core to the goal of interoperability is a defined clinical data set that is appropriate to support treatment, payment and operations for all who need to exchange such information. Standards which allow for consistency among the format and content of data, but also allow for flexibility for additional information as needed and based upon the discretion of the provider to support the healthcare process is the most appropriate "amount".

P 33 – Regarding the GUI interface, the report raises concerns about the variety of interfaces. While standardization has some benefits, the report also talks about the need for customization by provider type and system. There is an inherent contradiction between standardization and customization. EHNAC has seen scenarios where standardization inhibits advancements and innovation. The Department must carefully derive the most appropriate balance of provider workflow preference (especially across different specialties) with standardization of the interface.

P 33 – The discussion of the physical environment must also consider the security of the computer system and equipment as well as ease of use. Patient privacy must be protected, and the physical environment whether in the office, or as a virtual worker, is a key element of HIPAA Privacy and Security requirements.

P 34 Authentication is a critical piece of the security structure. While ease of use is one consideration, the strength of authentication must be considered. Additionally, each type of authentication has its strengths and weaknesses, and we would not expect see any one type implemented universally – especially as new techniques, technologies and best practices become available.

P 35, and Recommendation 1 on P 56 – User training. We agree that initial and ongoing training for users is critical for effective EHR usage. The HIPAA Security Rule requires regular security training for all employees. We recommend that HHS consider a requirement for EHR training as part of the Promoting Interoperability programs for hospitals and other providers. All workforce members should be comfortable with the data they handle, including basic functionality and safeguarding protocols.

P 36, The section on eCQMs brings up the issue that EHRs are being used for many tasks besides their initial intent, the recording of patient clinical data. This has complicated the systems as they take on these additional tasks. HHS may wish to look at streamlining the EHR systems and consider separating some functions so that clinicians are not faced with the burden of additional data (as long as that data is not needed to support the clinical treatment process).

P 46-47 – Good patient care requires complete and accurate patient documentation. EHRs should be built to implement appropriate documentation policies, not drive them. As stated above, HHS should determine required documentation policies, but allow the providers and EHR vendors build processes which balance provider operational workflow with clinical protocols.

P 50 – The key issue with prior authorization is the process itself, not just making it more automated. Health plans and providers need to work together on that process improvement. The technology piece is less of the problem. If interoperability is used consistently across all who exchange data, the process itself should improve. Focus on improvement of the process, then leveraging technology should be undertaken.

P 54 Recommendation 4 – The physical environment is a key piece of the privacy and security protections that must be in place; the HIPAA Security Rule has an entire section of physical requirements. Safeguarding the PHI by applying privacy and security best practice policies, procedures and technical controls should remain the utmost priority, with "ease of use" being secondary, although helpful to ease the provider burden.

P 56 Recommendation 2 – Costs of EHR implementation and support have been an ongoing issue. Planning for costs is important, but the industry should also look for ways to reduce costs thru shared training, simpler upgrades, consistent product functionality and other methods.

P 63 – 64, These strategies should be applied to all measures, not just the eCQMs.

EHNAC appreciates the opportunity to provide feedback on this RFI and stands available to assist with any specific questions and to participate in future endeavors.

Sincerely,

Executive Director, CEO

Cc: EHNAC Staff