DirectTrust®

November 1, 2023

[redacted]

Submitted electronically via https://cyberframework@nist.gov

SUBJECT: Comments to the Public Draft: The NIST Cybersecurity Framework 2.0

DirectTrust appreciates the opportunity to comment on this NIST Cybersecurity Framework Initial Public Draft to ensure guidance to industry, government agencies, and other organizations to reduce cybersecurity risks. In January 2023, DirectTrust announced that the Electronic Healthcare Network Accreditation Commission, EHNAC, had merged with DirectTrust. Both DirectTrust and EHNAC have provided healthcare data exchange and privacy/security comments to NIST for many years. Both non-profit organizations have similar missions and having joined forces strengthens our collective commitment to facilitate trust and broaden healthcare data exchange industry opportunities.

Relevant Background

DirectTrust™ is a non-profit, vendor-neutral alliance dedicated to instilling trust in the exchange of health data. The organization serves as a forum for a consensus-driven community focused on health communication, an American National Standards Institute (ANSI) standards development organization, an accreditation and certification body through EHNAC (the Electronic Healthcare Network Accreditation Commission), and a developer of trust frameworks and supportive services for secured information exchange like Direct Secure Messaging and trusted, compliant document submission.

The goal of DirectTrust is to develop, promote, and, as necessary, help enforce the rules and best practices necessary to maintain privacy, security, and trust for stakeholders across and beyond healthcare. In addition, DirectTrust is committed to fostering widespread public confidence in the interoperable exchange of health information while promoting quality service, innovation, cooperation, and open competition in healthcare.

- Through EHNAC, the DirectTrust accreditation and certification body, the organization promotes third-party trust concerning privacy and security as each candidate demonstrates through on-site review that specific standards are met for each program and can thus be "trusted" to handle such sensitive information across the healthcare continuum. With 20+ healthcare stakeholder-specific programs available across the industry, the following types of healthcare data exchange business models are addressed: Health Information Exchanges (HIEs), Electronic Health Networks/Clearinghouses (EHNs), and Financial Services Organizations (FSOs). EHNAC also certifies Electronic Prescription of Controlled Substances (EPCS) programs for vendors. Newer programs address the interoperable exchange of data, including a jointly administered program with HITRUST known as the Trusted Network Accreditation Program (TNAP). TNAP aligns with the ONC Trusted Exchange Framework and Common Agreement (TEFCA) requirements as well as the Trusted Dynamic Registration and Authentication Accreditation Program (TDRAAP), offered by EHNAC and UDAP.org. These programs are designed to facilitate endpoint trust for industry interoperability both for Covered Entities and non-HIPAA regulated entities. The majority of programs noted above have the NIST Cybersecurity Framework embedded as part of required criterion. These programs are considered meeting "Recognized Security Practices" as required by Public Law 116-321, known as the "HIPAA Safe Harbor Law".

DirectTrust (including EHNAC) has represented the data exchange healthcare industry for more than 25 years with a transparent and open governance process and the promotion of cost-effective independent third-party accreditation/certification services. The organization is engaged in several key initiatives that support safe and secure interoperability:

- Participation as a member of the Office of the National Coordinator's FAST Executive Committee and co-leader of the respective Testing and Certification Tiger Team.
- Member of the Board of the Sequoia Project/Recognized Coordinating Entity supporting TEFCA implementation. and interoperable data exchange
- Co-chair of the Interoperability Matters Leadership Council
- Member of the Healthcare Sector Coordinating Council (HSCC), and
- Participation in the HHS 405(d) Cybersecurity Information Sharing Act (CISA) and Health Care Sector Coordinating Council (HSCC) since its inception, with contribution of articles, policies, and best practices for industry use.

<u>Comments</u>

DirectTrust has the following general comments for consideration:

- DirectTrust supports the emphasis on broadening the applicability of the framework and elevating governance. Making sure that those with senior-level responsibility set the cybersecurity strategy and monitor the program is key to a successful implementation.

- The detailed content and "how-to" approach of the framework is very helpful.

- The effort to broaden the reach of the framework and yet to become more detailed at the same time (by using the online tools for implementation examples) is promising. Setting policy and guidelines is best suited for NIST (as it does so well across so many stakeholder disciplines). However, the healthcare data exchange environment itself has unique and explicit needs, characteristics, features, and problems (just like every other sector of the economy). The industry needs to constantly provide detailed feedback and NIST needs to provide ongoing monitoring of this feedback, sector by sector in order to determine what needs to be generalized or scaled up.

- Suggestions of partners to facilitate the ongoing feedback mentioned above include but are not limited to:
  - The Health and Human Services 405d public/private collaborative on cybersecurity also includes practical charts, policies, procedures, and other materials focused on healthcare data exchange for smaller providers. Enterprise Risk Management tables/samples and scenarios addressing situations such as but not limited to ransomware and insider threat handling are published. These may be appropriate for cross-referencing or inclusion.
  - The Workgroup for Electronic Data Interchange (WEDi) has aided the healthcare industry in the past in the implementation of HIPAA and other regulatory requirements. Perhaps partnering with such an entity specifically to address niche areas like healthcare data exchange unique to the small provider (including solo providers through city county and local hospital systems) would be an avenue to consider. WEDI is also a designated advisor to the HHS Secretary.
- Leveraging the above initiatives, a "cybersecurity starter package" specifically aimed at local providers including city and county-level hospitals, utilizing the efforts of the 405(d), could be prepared specifically for healthcare data exchange.
- DirectTrust believes the use of the online tool for the detailed implementation examples provides a structure, but that specific efforts to partner with other entities who focus on the healthcare data exchange environment will be helpful. The online tool addressing implementation examples should be user-friendly, easy to navigate, and easy to filter and sort even for those not well-versed in cybersecurity. The use of vignettes, use cases, and examples that are easy to retrieve for smaller providers will be most helpful. These could begin with a simple statement such as "This is how a solo dentist chose to solve the cybersecurity problem of xxx". Providing materials specific to smaller organizations such as secondary tools and charts will ease adoption, and analysis and provide additional audit guidance.

DirectTrust has the following specific comments as they relate to healthcare data exchange for consideration:

- In general, the CSF 2.0 version addresses many cybersecurity-related topic areas, however, additional guidance and examples in the areas of ransomware, use of third-party applications, and the incidence of “insider threat” will benefit users.

- Third-party risk management terminology can be expanded to include those downstream entities such as third-party applications, cloud service providers, and others providing data handling services along with the associated risks.

- Regarding IDAM 07 within Asset Management, emphasize the importance of beginning with the identification and classification of the data that is handled. This ties in with the Office for Civil Rights recommendations on conducting HIPAA Risk Analysis (in accordance with the HIPAA Security Regulations) where the “handling” (creation, receipt, maintenance, and transmission) of all Protected Health Information is the core of the evaluation of the asset/function. Perhaps this can be built into implementation examples, but the need to begin with the information/data to be protected by the organization is key to the comprehensive evaluation of assets.

- Regarding PRAT- Awareness and Training – Perhaps also noted for the implementation process, but the healthcare data exchange industry has largely adopted a step to ensure workforce members adhere to organizational policies and procedures by requiring an ongoing “acknowledgment” (in addition to routine reminders/cheat sheet documents) to raise awareness and to ensure that such required documents are understood by each workforce member in an effort to help spread the risk of non-compliance across the organization.

- Continue to tighten and/or further strengthen the linkage between the use of KPIs related to cybersecurity and governance. For example, activities should be “rolled up” and presented regularly at the senior leadership level as they are integrated into measurement and tracking via the use of statistics and charts.

DirectTrust appreciates the opportunity to participate as part of industry feedback on this important document.

Respectfully submitted,

Scott Stuewe
President and CEO, DirectTrust