

National Working Group to Standardize the Identification of Sensitive Data Elements to Support Patient Privacy

Marianne Sharko, MD, MS¹, Hannah Galvin, MD, FAAP², Susan J. Kressly, MD, FAAP³, Joseph H Schneider, MD⁴, Fabienne Bourgeois MD, MPH⁵, Feliciano (Pele) Yu, MD⁶, Matthew Hong, MHCI⁷, Lauren Wilcox, PhD⁷, Jessica S Ancker, MPH, PhD¹

1. Department of Healthcare Policy & Research, Weill Cornell Medical College, New York, NY, 2. Lahey Health, Burlington, MA, 3. Kressly Pediatrics, Warrington, PA, 4. UT Southwestern Medical Center, Dallas, TX, 5. Harvard Medical School, Boston Children's Hospital, Boston, MA, 6. Arkansas Children's Hospital, Little Rock, AR, 7. School of Interactive Computing, Georgia Institute of Technology, Atlanta, GA

Problem addressed:

In this age of electronic medical information collection, storage, analysis and exchange, it is important to protect patients' rights to privacy over sensitive medical information. State laws and medical center policies governing privacy protection can vary and provide a complex backdrop for the standardization of sensitive data. It is important to consistently identify sensitive information in order to prevent the unintentional sharing of information through the electronic health record (EHR), patient portal or health information exchange (HIE).

Without standardization, medical organizations are left on their own to define the types of information identified as sensitive, and in need of heightened protection. This results in varying lists of sensitive data which can leave patients vulnerable to breaches of privacy. This is of particular importance to vulnerable populations, such as adolescents, patients seeking mental health or sexual reproductive care, or patients using proxies to manage their healthcare. HIE can provide challenges to data protection due to differing privacy policies. With limited ability to identify sensitive data in the EHR, many systems rely on individual professionals to provide this protection. The informatics community and industry have found it difficult to address these challenges due to its complexity and lack of business and/regulatory drivers. However, it continues to be a clinical problem that impacts patients and providers daily.

Purposes of the working group:

A previous study found that many chief medical information officers (CMIO's) welcome more formal assistance in the identification and control of sensitive data; however, national guidelines should be thoroughly vetted.¹ The established standards should align with recommendations from medical associations and state laws, and should be adaptive enough to accommodate differing patient needs. We have developed a working group through a snowball recruitment process to define the problem and to brainstorm potential solutions. This group, working with the AAP Council of Clinical Information Technology and the Child Health Informatics Center includes pediatricians, adolescent specialists, CMIO's, informaticists, researchers, and human-computer interaction specialists.

A primary aim of the group is to develop industry and expert consensus around recommendations for privacy protections at the data element level, a granularity previously thought to be too complex to address, yet which is necessary to support clinical use cases. Currently a clear list of sensitive data does not exist. To that end, we have begun categorizing data elements into levels of sensitivity through a small group consensus process to identify those with heightened privacy protection needs, such as from mental or sexual histories. We have also developed clinical use cases to demonstrate the need for standards development. Communication with vendors to delineate privacy expectations and create functional standards will help motivate electronic advancements, provide long-term consistency, and garner support from the ONC through their rule-making process. We look forward to sharing our processes, sensitive data lists and use cases to advance this conversation so that patients and families can benefit from the accurate exchange of information with confidence that their wishes regarding data privacy are respected.

References:

1. Sharko M, Wilcox L, Hong MK, Ancker JS. Variability in adolescent portal privacy features: how the unique privacy needs of the adolescent patient create a complex decision-making process. *J Am Med Inform Assoc.* 2018;25(8):1008-1017.