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

Marianne Sharko, MD,MS[1], Susan J. Kressly, MD,FAAP[2], Feliciano (Pele) Yu, MD[3]
Fabienne Bourgeois, MD,MPH[4], Joseph H Schneider, MD[5], Jessica S Ancker, MPH,PhD[1],
Matthew Hong, MHCI[6], Lauren Wilcox, PhD[6], Hannah Galvin, MD,FAAP[7]

1 Department of Healthcare Policy & Research, Division of Health Informatics, Weill Cornell Medical College, NY, 2 Kressly Pediatrics, Warington, PA,
3 Arkansas Children's Hospital, AR, 4 Harvard Medical School, Boston Children's Hospital, MA, 5 UT Southwestern/Parkland Hospital in Dallas, TX,
6 School of Interactive Computing, Georgia Institute of Technology, GA, 7 Lahey Health, Burlington, MA

Background

- In this digital age of medical information collection, storage, analysis and exchange it is important to protect sensitive medical information
- Laws governing privacy protection for vulnerable populations vary from state to state and provide a complex backdrop for the standardization of sensitive data identification.
- Currently there is limited technological capabilities to reliably identify all sensitive data in an EHR.
- It is important to identify to prevent unintentional sharing of info through the EHR, patient portal or health information exchange.
- Without standardization, medical organizations are left on their own to identify sensitive data in need of heightened protection.
- Inconsistency can leave vulnerable populations vulnerable to breaches of privacy.
- Health information exchange can provide a challenge to sensitive data protections since medical information may be subject to differing privacy policies depending on the medical center and the state laws. A patient may disclose sensitive medical information in one setting, only to find that this information no longer protected in a different setting.
- Many CMIO's feel that more national guidelines would need to be thoroughly vetted by those actively involved in the care of vulnerable populations.[1] Guidelines would need to be adaptive enough to accommodate differing state laws and community expectations.

Working Group Efforts

- Discussion to determine basic common goals of privacy for vulnerable populations
- Identify and stratify sensitive data elements
- Develop clinical use cases to demonstrate the need for standard development
- Work with **AAP, Council of Clinical Information Technology and the Child Health Informatics Center,** and utilize input from various stakeholders, including professional society members, pediatricians, adolescent specialists, informaticists and human computer interaction specialists
- Communicate with vendors to delineate privacy expectations and to promote the creation of functional standards in EHR systems with sufficient granular control to be able to accurately and reliably identify information and provide privacy protection

Vulnerable Populations

- Adolescents
- Patients with mental health, substance abuse data
- Patients with sexual and reproductive health data
- Patients with intimate partner violence data
- Elderly with health proxies
- Developmentally challenged with health proxies
- Foster care system members

Adolescents & Portal Access

- Adolescence is a time when patients are approaching autonomy, both developmentally and legally, yet they are still considered minors
- Patient portals enable improved access to providers and medical information.
- However, federal policy, state law, and community norms are not consistent regarding adolescent healthcare and privacy.
- In the absence of national guidelines, medical centers encounter serious challenges when developing policies about patient portal access

AAP Policy Statement of 2012

Health information systems currently lack the capability to allow for protection of the privacy & security of health information for minors.

Society for Adolescent Health and Medicine 2014

Design, implementation, and use of EHRs need to take into account the special needs of adolescents for access to health information and vigorous protection of confidentiality.

American College of Obstetricians and Gynecologists 2014

EHRs should be customized to accommodate the confidentiality needs related to minor adolescents and to comply with the requirements of state and federal laws.

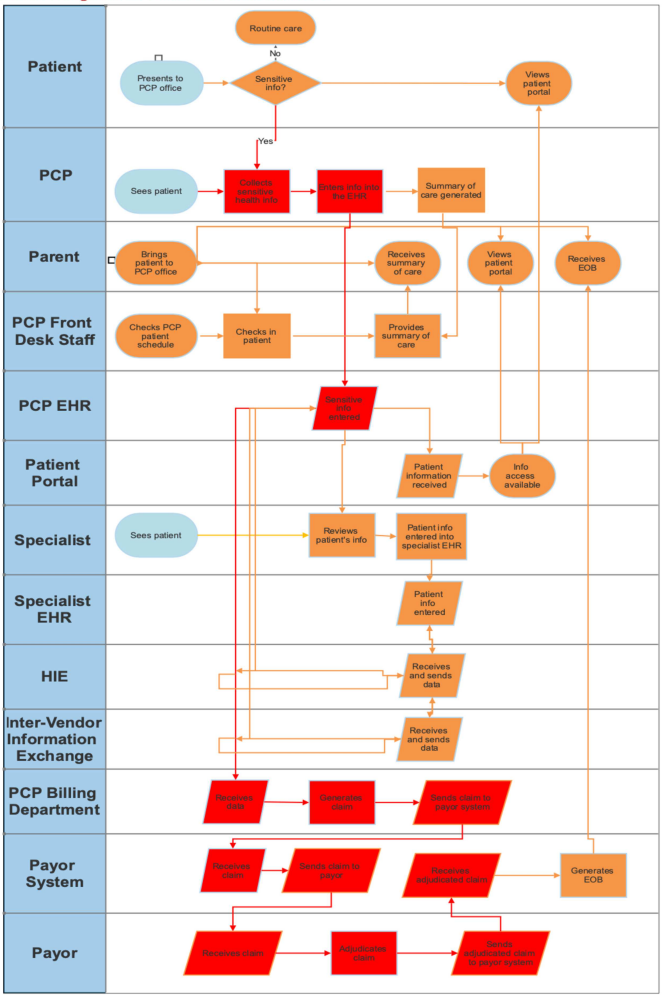
Swim Diagram Color Codes

- No sensitive information
- Potential sensitive information
- Definite sensitive information

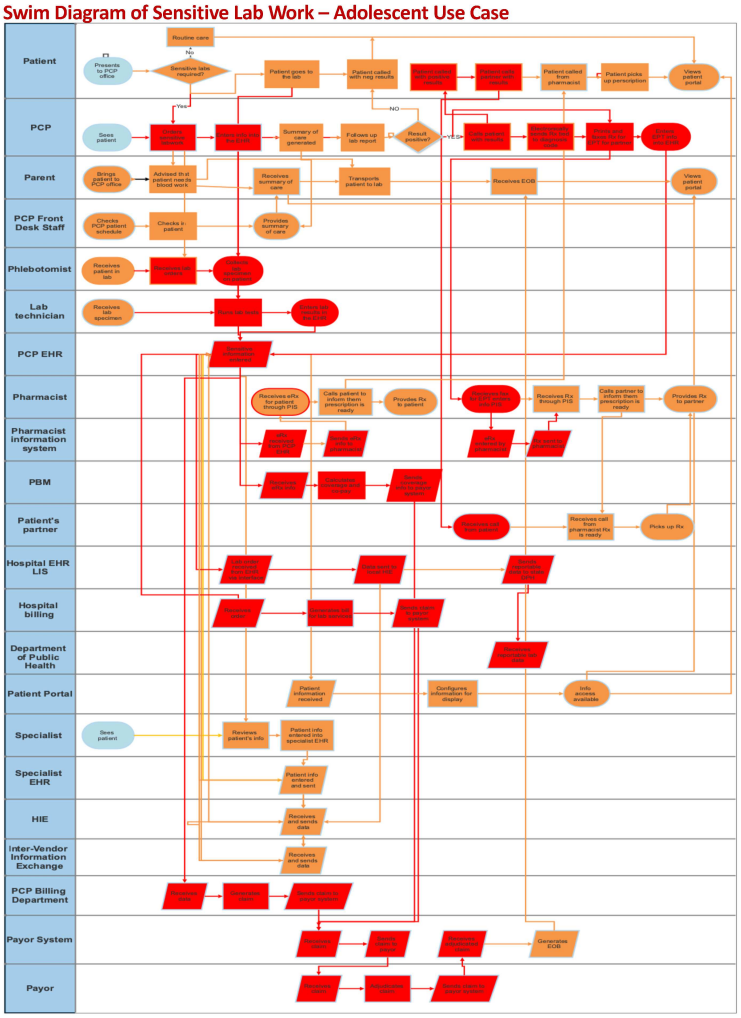
Adolescent Use Case

16 y/o female with PMH of asthma presents to her pediatrician for a well child check. Patient is sexually active with 1 male partner, using condoms "most of the time." She denies urogenital complaints. She requests a prescription for an oral contraceptive pill.
Pediatrician discusses contraception options, risks and benefits, and prescribes low-dose combination pill, recommending continued use of barrier methods. Also sends urine gonorrhea/chlamydia.
The following day, chlamydia returns positive, gonorrhea negative. Clinician calls patient on cell phone to discuss dx, counsel, and call in azithromycin for patient and expedited partner therapy for her boyfriend. Clinician records diagnosis of A74.9 on patient's problem list and ties it to the azithromycin Rx.
The patient has access to her health information via the patient portal. Her parents also have unrestricted proxy access to her health information via the portal. The patient expresses that she does not want any information related to the visit seen by her parents (including related to labs, prescriptions or on the Explanation of Benefits), and does not want this information sent to the local Health Information Exchanges or shared in other clinicians outside of the practice.

Swim Diagram of Sensitive Information



Swim Diagram of Sensitive Lab Work – Adolescent Use Case



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.