

**HIT POLICY COMMITTEE MEETING
SEPTEMBER 18, 2009
COMMENTS FOR CONSIDERATION**

Planned Parenthood Federation of America strongly supports federal efforts to accelerate the appropriate adoption and use of health information technology (HIT) to enhance health care delivery and patient outcomes, while maintaining high standards regarding the privacy and security of patient health information. We very much appreciate the opportunity to provide comments to the HIT Policy Committee on the important topic of privacy and security for HIT and health information exchange (HIE).

Planned Parenthood Federation of America is a national not-for-profit organization that provides support services to 93 separately incorporated affiliates that operate more than 850 reproductive health care centers in almost every state. Each year, Planned Parenthood health centers provide reproductive health care, including routine gynecological exams, breast and cervical cancer screenings, contraceptive services, abortion care, STI testing and treatment, and HIV testing and education, to more than three million patients — the vast majority of whom are at or below 150 percent of the federal poverty level.

Privacy and Security Across the Spectrum of Planned Parenthood Health Care Delivery

As America's most trusted provider of reproductive health care, Planned Parenthood understands the importance of privacy and security as the foundation of health care delivery. We have more than 90 years of experience in providing comprehensive reproductive health care in settings that preserve and protect the essential privacy rights of individuals and in advocating for public policies and procedures to guarantee these rights and ensure access to reproductive health care.

Consideration of privacy and security issues in the context of Planned Parenthood care may test the boundaries of the HIE debate. Many patients come to Planned Parenthood specifically to ensure that their family, insurer, employer, and/or their other health care providers do not know that they have obtained care. Often the stakes are high, as release of this information might compromise the patient's personal safety or lead to acts of discrimination. In addition, patients may defer or delay seeking care if they are concerned that their privacy may be compromised. Given the importance of timely preventive health care and any needed follow-up, the earlier Planned Parenthood is able to provide confidential care for our patients, the better the individual and public health outcomes will be.

The privacy and security concerns inherent in Planned Parenthood care do not stop with our patients. Staff and clinicians risk their personal safety by providing reproductive health care. An extreme example is the recent murder of Dr. George Tiller (while he was not a Planned Parenthood provider, he was an integral part of our community). Many of our providers face threats in the health centers and in their homes, and Planned Parenthood must protect their privacy as well as that of our patients.

Finally, we are frequently targeted by organizations and individuals, including government officials, with political agendas to use patient information without their consent. Indeed, in one recent instance, the Kansas Supreme Court chastised the former Kansas attorney general for his handling of medical records as, “inexcusable.... [demonstrating] that he is interested in the pursuit of justice only as he chooses to define it.”¹

Demonstrated Commitment to Widespread Adoption of HIT/HIE

With hundreds of health centers nationwide, Planned Parenthood understands the need for and value of networked HIT for the efficient operation of health care centers, enhanced delivery and coordination of care, and patient support. We further understand the value in being able to analyze data and trends on a national level to improve patient safety and public health outcomes and to conduct nationwide clinical research to advance best practices and evidence-based care delivery at all Planned Parenthood health centers.

To demonstrate our collective commitment to these goals, in 2007 Planned Parenthood affiliates jointly agreed to move toward the adoption of standardized clinical information systems in all Planned Parenthood health centers over a five-year period. The challenges and nuances of federal and state privacy and security requirements that pervade delivery of care at Planned Parenthood have been and continue to be addressed by our affiliates as they move forward with adoption of electronic health records.

Scenarios for Consideration

In developing these comments on privacy and security considerations for the use and disclosure of health information in a networked HIE environment, with implications for the secondary use and stewardship of such data, Planned Parenthood brings to bear its years of experience as a provider of highly sensitive, confidential health care. The obvious bears stating here: We are at the point when we must address significant concerns about the use and disclosure of sensitive data. Until now, many efforts to establish HIEs have postponed addressing these issues and moved forward by excluding sensitive data. If we continue to sidestep these issues, we will not only shortchange women, men, and teens who use reproductive health care, we may in fact endanger their lives. Our patients can and should realize the benefits from HIT adoption and HIE. We are prepared to work with you to create solutions that bring the benefits of HIT and HIE to even the most sensitive patient populations.

In order to further illustrate our perspective and to give context for the discussion of privacy and security considerations that follows, we present four patient care scenarios for consideration by the HIT Policy Committee. These are provided to put in sharp relief the fact that although information regarding much of the care provided in our health centers will be sufficiently protected under current mainstream HIE privacy and security policies and practices, there are instances in which heightened protections are essential, or the consequences can be life changing, or even life threatening.

¹ *Comprehensive Health of Planned Parenthood v. Kline, et al.*, 197 P.3d 370 (Kan. 2008).

The scenarios:

Scenario One: *A 17-year-old high school senior obtains family planning services to prevent pregnancy, so that she can pursue her dreams of college and a medical career. Her parents disapprove of premarital sex and have told her that if they ever found out that she was having premarital sex they would ostracize her and force her to leave the family home. The state she lives in allows family planning services to be provided to minors without parental involvement, and this minor has indeed obtained confidential care. The minor becomes ill with fever and her mother, suspecting swine flu, takes her to the emergency room. Under the same state's law, the parent must consent to the care the minor will receive at the hospital. When the hospital provider consults the HIE for medical information on the minor, how can we ensure that the health information related to the confidential family planning services will not be made known to the parent?*

Scenario Two: *A 20-year-old woman whose entire family uses the same family medicine provider contracts a sexually transmitted disease. She does not want her doctor to know and is worried that he will not keep this information confidential. She gets testing and treatment from Planned Parenthood. How can we ensure that a patient may selectively release information only to/from certain providers?*

Scenario Three: *A 36-year-old woman, who has previously had an abortion at a Planned Parenthood health center and has not elected to keep this data confidential goes for care in a community hospital emergency room with an elevated heart rate where a clinician, who is an anti-choice activist, sees her medical history, including the name of the physician who performed the abortion. Who determines what information is legitimately needed?*

Scenario Four: *A 39-year-old woman, in an abusive relationship, comes to Planned Parenthood to receive reproductive health care. She is concerned about using her insurance since she does not want her abusive husband to see an explanation of the care she received. How can the scope of health information disclosure for claims processing be structured to accommodate for patient confidentiality concerns with primary or secondary payers?*

Planned Parenthood health centers, as well as other providers of sensitive health care, have a unique role in the continuum of care. Our patients expect — not unreasonably — not only high-quality reproductive health care, but that their privacy will be safeguarded and that their well-being will not be put in jeopardy as a result of receiving care at Planned Parenthood. The decision of the Planned Parenthood health centers to adopt HIT and participate in HIE must not violate that trust.

We move forward with the assumption that sensitive data **will** be part of data exchange. Thus, what are the implications?

Discussion of Privacy and Security Considerations for HIT and HIE

As the patient care scenarios set forth above clearly demonstrate, privacy concerns in the context of reproductive health and other sensitive care are often situational in nature and grave in consequence. As a result, developing a comprehensive privacy and security framework for HIE will be a complex

undertaking that will continue to evolve in the coming months and years. We believe that continued conversations and detailed analysis will be required to ensure that all risks, including for the most sensitive situations, are appropriately addressed. However, we believe that the following core issues, if addressed at the outset, will help to build a strong foundation of privacy and security protections to govern the use, disclosure, secondary use, and data stewardship of health information within an HIE. We raise these issues here, and propose to work with you to explore specific situations and circumstances — yet other scenarios — through which risk assessment can be conducted and necessary protections developed.

Locus of Authority: Within a networked HIE environment, the locus of authority should remain vested with the provider and patient, to protect the original understandings developed between patient and provider in the context of delivery of care.

Keeping the locus of authority for release of information nearest to the point of care will help ensure that HIE is done in compliance with state and local laws, under which the provision of medical services is largely regulated. It will also permit the provider to exert the same level of professional judgment for the delivery of health care in an electronic environment as in a more traditional environment.

The HIPAA Privacy Rule recognizes that decision-making authority must be vested at the provider level for uses and disclosures that are central to health care delivery and the operation of a health care delivery system, but that individuals should be granted authority to protect their information against more ancillary uses. The HIPAA Privacy Rule further recognizes the importance of allowing providers the discretion to determine when uses and disclosures are necessary and appropriate for legal compliance, public health activities, health oversight activities, legal proceedings, and law enforcement purposes.

While HIPAA recognizes the importance of these activities and allows for disclosures in these circumstances without requiring patient authorization, HIPAA does not mandate information exchange in any of these circumstances. In fact, HIPAA mandates disclosure in very limited circumstances, such as when the patient requests his or her own health information.

Preserving these principles in a networked HIE environment is critical to protecting not only the privacy of individual health information, but also in protecting an individual's right of access to comprehensive health care, including the full range of reproductive health care, without unnecessary intrusion.

Mechanisms to Prevent Misuse: HIE must be grounded in principles of acceptable use that are designed to facilitate improvements in health care delivery and eliminate opportunities for inappropriate access. Acceptable use policies must address and eliminate inquiries and requests for access to health information that are prompted by motivations outside the continuum of care.

Policies must address not only inappropriate requests that are motivated by “economic opportunity” — as evidenced by highly publicized instances of exploitation of celebrity health records or misuse of health records to perpetrate financial fraud — but also inappropriate requests that are motivated by “political opportunity.” Planned Parenthood has a long history of defending its patients' medical records and providers' identities against the prying inquiries of those outside the patient-provider relationship, ranging from family members to employers to states' attorneys general. In order to

provide a safe and reliable environment for HIE, policies must be developed to ensure that HIE is not exploited for economic, political, or other inappropriate purposes at the expense of individual and provider privacy.

Role-Based Permissions and Limitations on Scope of Information Exchanged: Participants in HIE must disclose and/or use only the requisite amount of information necessary to accomplish the specific purpose of the exchange. HIE must further tailor the scope of information exchanged to the role of the requesting party. For example, the relevant information for a patient who has experienced a post-procedure complication would include the medical history and procedure notes, whereas, the information required for a mammogram referral would not require detailed history. The HIPAA Privacy Rule sets forth the paradigm of “minimum necessary” as a means of preventing unnecessary use and disclosure of health information. HIE policy must be grounded in similar requirements, developed mindfully to account for the expanded roles and responsibilities of HIE participants.

Limitations on Further Use: HIE must dictate not only the scope of the rights of HIE participants to request and access health information, but also the responsibilities of HIE participants with respect to the health information after exchange. Given the potential for wide variation in the types of participants in HIE and their professional and/or legal obligations to ensure that exchanged information is treated confidentially and not misused after exchange, clear standards must be developed to clarify these obligations for all participants and for the various types of acceptable use of HIE. Special attention must be paid to further use of sensitive information, as patients will expect that the confidential nature of the care they receive at trusted providers like Planned Parenthood will follow their health information wherever it goes.

Accountability: The framework for protecting privacy within the context of HIE must include not only mechanisms such as those described above to protect privacy proactively before violations occur, but must also include comprehensive structures and systems to monitor compliance and to detect, report, and penalize noncompliance in a manner that is commensurate with the nature of the violation. HIEs must provide a stringent set of physical, administrative, and technical safeguards, including comprehensive and granular logs across all aspects of system usage, and be required to frequently audit logs for patterns of unusual or suspicious behavior and to take timely action to report and remedy any misuse and institute measures to prevent further violations. Consequences for violation of HIE privacy and security provisions should be substantial and penalties should be tailored to the nature of the misuse, with heightened civil and criminal liabilities and professional sanctions imposed for misuse of sensitive information.

Conclusion

To be successful and realize the full promise of a networked HIE environment, HIE systems will require robust and widespread adoption within the provider community, which can only be accomplished through building patient trust and confidence in HIE privacy and security protections. As a national provider of high-quality, cost-effective health care to underserved populations, Planned Parenthood strongly desires to participate fully in and realize the myriad of benefits promised by HIE. As a core component for measuring meaningful use of HIT, policies for privacy and security must be developed to

ensure that HIE fully protects individual privacy across the spectrum of health care delivery, including the vulnerable populations served by essential community providers like Planned Parenthood. We thank you for the opportunity to contribute to the national conversation on these important issues.

Please contact Eileen Twiggs with any questions at (212) 541-7800.