This report is part of the RAND Corporation research report series. RAND reports present research findings and objective analysis that address the challenges facing the public and private sectors. All RAND reports undergo rigorous peer review to ensure high standards for research quality and objectivity.

ARROYO CENTER and RAND HEALTH

Patient Privacy, Consent, and Identity Management in Health Information Exchange

Issues for the Military Health System

Susan D. Hosek, Susan G. Straus

Prepared for the United States Army

The research described in this report was sponsored by the United States Army Medical Research and Materiel Command, Telemedicine and Advanced Technology Research Center (TATRC). It was conducted jointly by RAND Health and RAND Arroyo Center, a federally funded research and development center for the U.S. Army.

Library of Congress Cataloging-in-Publication Data

Hosek, Susan D.
Patient privacy, consent, and identity management in health information exchange : issues for the military health system / Susan D. Hosek, Susan G. Straus.
pages cm
Includes bibliographical references.
ISBN 978-0-8330-7790-5 (pbk. : alk. paper)
1. Medical records—Access control—United States. 2. United States—Armed Forces—Medical care. 3. Medicine, Military—United States—Information services. 4. Medical informatics—United States. 5. Information storage and retrieval systems—Medical care. I. Straus, Susan G. II. Title.

R864.H67 2013
610.285—dc23 2013015711

Published 2013 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
RAND URL: http://www.rand.org
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Summary

The Military Health System (MHS) and the Veterans Health Administration (VHA) have been among the nation's leaders in health information technology (IT), including the development of health IT systems and electronic health records (EHRs) that summarize patients' care from multiple providers. Health IT interoperability within MHS and across MHS partners, including VHA, is one of ten goals in the current MHS Strategic Plan; the ability to exchange health information between military and nonmilitary health care providers is especially important in light of the role played by civilian providers in MHS's TRICARE program, which provides care to 9.7 million beneficiaries.

The MHS has taken several steps toward achieving improved interoperability, including collaborating with the Department of Veterans Affairs (VA) to develop an integrated EHR, a virtual lifetime electronic record (VLER), and Joint Federal Health Care Centers. The MHS is also seeking to develop a research roadmap to better coordinate health IT research efforts, address MHS IT capability gaps, and reduce programmatic risk for enterprise projects in the MHS. This report contributes to that effort by identifying key research and policy issues involving patient privacy, patient consent, and patient identity management as relevant to health information exchange (HIE) in the Department of Defense (DoD). Our study used a multimethod approach consisting of a review of policy regarding privacy, patient consent, and patient identity management; a literature review on these topics as relevant to the MHS; and semistructured telephone interviews with 31 subject-matter experts. We use a sociotechnical framework to organize our findings and to suggest topics for future research.

Privacy of Individual Health Information

The shift from paper medical records to electronic records raises new concerns about privacy, the protection of which is key to patient consent and identity matching.

Legislation and Policy

The federal government mandated the protection of protected health information (PHI) by health care organizations 16 years ago, through the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA established federal standards designed to safeguard individual health records while allowing for the exchange of information to ensure the quality of health care and public health. The HIPAA Privacy Rule regulates the disclosure and use of individuals' PHI that is or has been maintained or transmitted electronically by covered health care entities. Some states have copied the HIPAA provisions into state law, sometimes adding restrictions on the disclosure of PHI relating to especially sensitive areas such as mental health or the human immunodeficiency virus (HIV).

The Department of Health and Human Services (DHHS) has developed a framework identifying privacy protection and information security principles that health information organizations (HIOs) should follow. Among the principles outlined are individuals' right to access their information through simple and timely means; the right to dispute the accuracy or integrity of their information and correct it or have their dispute recorded; and the need for transparency about policies, procedures, and technologies that affect patients or their PHI. Similar frameworks have been developed by other public and private health care organizations.

Considerations for DoD and VA Concerning Privacy

There is widespread consensus on the principles that should guide HIE, including the need for consent for HIE and accuracy in linking EHR information to patients. However, there is less consensus about the specific approaches used to implement these principles. The goal of

policy is to design approaches that find the right balance between the beneficial use of EHRs and privacy protection.

Patient Consent

Patient consent or authorization for HIE is central to the issue of privacy, yet there is often ambiguity and controversy about the meaning of *consent* and the mechanisms for obtaining it. For example, responses to requests for public comment on the proposed HIPAA rule revealed that many individuals felt that they "own" their health records and should be asked for permission to release PHI for every request. Nonetheless, survey data indicate that a large majority of Americans support HIE to improve health care.

Consent Regulations

There are a number of federal regulations governing consent requirements for use and disclosure of PHI. The HIPAA Privacy Rule attempts to create a balance between safeguarding individuals' privacy and allowing for the disclosure and use of information to promote health care quality and efficiency. There are several situations or activities, including treatment, payment, or health care operations, for which covered entities can disclose PHI without first obtaining authorization from patients. Patients must be allowed to request restrictions on the disclosure of their information for permitted uses, but covered entities are not required to agree to these requests. Other federal regulations pertaining to consent for HIE govern the disclosure of clinical laboratory results, substance abuse treatment program records, and records of treatment for drug abuse, alcohol abuse or alcoholism, infection with HIV/AIDs, and sickle cell anemia by the VHA.

There are also myriad state laws regarding disclosure of PHI. The central issue with respect to patient consent is that electronic transmission facilitates the exchange of information across states, yet states have different disclosure requirements. Providers accessing information on a patient from another state must adhere to the disclosure requirements

of that state, which are likely to differ from and may conflict with the requirements in their state.

Consent Principles

Valid, informed consent consists of five elements: disclosure, capacity or competence, understanding or comprehension, voluntariness, and consent or decision. There are also multiple models of patient consent, ranging from *no consent*, in which HIE occurs automatically (which applies to active duty personnel), to various *opt-out* (in which HIE occurs by default) and *opt-in* (in which HIE requires written authorization) models. Most health exchange initiatives use opt-out consent at the provider or organizational level, and while both opt-in and opt-out consent can be implemented poorly, it is more difficult to ensure disclosure, capacity, and understanding for all patients using an opt-out approach. As a result, opt-out approaches may not reflect voluntary decisionmaking on the part of patients.

Recently, approaches to obtaining patient consent have tended to shift control of the process from providers to patients. Patient- or person-centric approaches, in which each patient is given a unique identifier and then accesses a single location to specify their preferences for HIE nationwide, offer numerous benefits, but also pose challenges. Centralized consent offers consumers control over who gets their PHI, for what purposes, and over what time frame. The approach also eliminates the need for providers to maintain separate records of patients' consent preferences. However, consumer-centric approaches require providers to have the means to store and access the consent service ID in their systems, and successful adoption depends on a variety of sociotechnical factors, including patients' willingness to manage their own consent data. If a patient puts restrictions on the content of the health information that can be exchanged, the provider's system must be capable of granular HIE (which limits data access and use based on factors such as the recipient, purpose, duration, and content of patient health information) or the provider must be willing to filter the patient's data manually.

Considerations for DoD and the VA Regarding Patient Consent

We anticipate that a number of changes in mechanisms for consent will be needed to support the VLER:

- DoD will need the capacity to record and implement patients' restrictions on the disclosure of PHI when they are approved under the current opt-out procedure.
- Retaining PHI from non-DoD providers will require implementing any disclosure restrictions on secondary disclosure. Current methods for granular consent are in their infancy.
- Research on the design and usability of automated text processing to redact restricted patient information, particularly in unstructured data such as clinical notes, is needed.

We expect that it may be difficult to proceed with VLER without a meaningful consent procedure that reflects the principles proposed by the Office of the National Coordinator for Health Information Technology's HIT Policy Committee "Tiger Team" (which call for "meaningful, revocable" consent for HIE other than direct provider-to-provider exchange). Although HIPAA allows providers to share patient health information for treatment, payment, and operations without patient authorization, we expect that many civilian providers may not be able or willing to do so. DoD may conclude that the best approach is to follow the VA in developing a patient consent management system for non–active duty beneficiaries.

To be meaningful, the consent procedure must adequately inform patients about the choices they have and the consequences of those choices, and the procedure must be conducted in a manner that ensures that consent is entirely voluntary. If DoD determines that there should be some kind of consent for HIE through VLER, research is needed to guide decisions about the type of consent, beneficiary outreach and education, and the procedure(s) to be followed.

Proactive research, carried out in the unique context of the military, would inform the development of future consent policy and the design of next-generation health IT systems. Additional topics for a research agenda on patient consent would include:

- pilot tests of patient consent management systems in clinical settings to assess their uptake and effectiveness
- analyzing and designing workflows to administer informed consent; ensuring that it is meaningful or valid in terms of disclosure, capacity, understanding, and voluntariness; and verifying consent for HIE at the point of care.

Patient Identity Management

Key issues involved in patient identity management include the identifiers to be used to link individual patients to their PHI and the approach used to identify an individual patient across multiple health care organizations.

Choice of Identifiers

PHI can be linked to individual patients through a number of identifiers, such as name, address, email address, phone number, or a unique patient identifying number (e.g., Social Security number [SSN]). Nonunique, out-of-date, or incorrect identifiers can lead to errors, including false negatives (failure to find a patient's information when it in fact exists) and false positives (finding information that is not, in fact, the patient's).

Identity Matching

Identity matching is the process used to identify the same individual across health care organizations using the specified identifiers for HIE. Numerous methods are available, from simple deterministic algorithms that require an exact match on the specified identifiers to highly sophisticated probabilistic, hierarchical algorithms in which a threshold must be set to establish a match.

Patient Matching Approach

Together, the choice of identifiers and a matching algorithm constitute a patient matching approach. Often, deciding which approach to use

means trading off between the false positive and false negative rates. Approaches that have a very low probability of matching to the wrong person also often lead to an increase in false negatives—not successfully matching to information available from other providers. Maximizing the successful match rate often comes at a cost of increasing the false positive rate—linking to the wrong patient information. Unique and accurate patient identifiers can lower both types of errors, as can more effective matching algorithms.

Without a national system of unique patient identifiers, patient identity matching for HIE poses difficult challenges. Even if a unique patient identifier were established, the potential for errors in recording it would require additional matching on other patient identifiers to ensure that the right patient's information is being exchanged. Considering the different combinations of patient identifiers that are potentially available and the many algorithms that can be adapted to this use, the number of patient identity matching approaches is very large.

Although studies have examined the different outcomes of matching approaches based on types of identifiers and matching algorithms, none of the research has been conducted in a functioning HIO with multiple providers. The studies use either simulated or proxy patient indexes and researchers instead of HIO managers to implement the matching algorithms. Thus, the literature provides very limited real-world information on which to base a choice of patient identifiers, matching algorithm, match criteria, and manual review of the results of automated matching.

Considerations for DoD and VA Regarding Patient Identity Management

More research is needed to assess the cost-effectiveness of the different options in practice, using actual patient registries or electronic medical records and the business processes that providers and HIOs are likely to sustain over time. DoD and VA could inform their own choices and contribute valuable information to guide others through investigation of the performance of promising approaches for nationwide implementation of VLER for all beneficiaries, including military family members:

- The research should evaluate to the maximum extent possible the performance of different approaches in matching at the scale that will be required for VLER at the national level once more civilian providers participate in the MHS's health network.
  - The research should use actual identifying data from the Person Data Repository, test performance at scale, and pilot promising approaches in the clinical setting.
  - The research should measure the trade-offs among key performance technical outcomes, including time needed to complete a patient information request, false negative and positive rates, and the expertise and resources needed for development and maintenance of the matching approach.
- A parallel line of research should focus on other issues related to implementation within organizations, such as work processes at the facility and system levels for ensuring the accuracy of patient identifying information, procedures at the clinical level that increase the efficient retrieval of electronic information from other providers to support patient care, and best practices for checking that the information received is for the right patient and is accurate.

As with patient consent, there are policy issues to resolve within organizations and at the federal and state levels regarding the type of identifiers that can maintain patient privacy.

Finally, following a sociotechnical approach, it is important to consider how technical, social, and organizational factors work together. Addressing isolated issues regarding patient identity management and consent will not be productive; research and implementation needs to address multiple factors and their interactions in supporting successful HIE.