HEALTH INFORMATION TECHNOLOGY & PRIVACY

American College of Physicians
A Position Paper
July 2011

ACP American College of Physicians℠
INTERNAL MEDICINE | Doctors for Adults

Health Information Technology and Privacy

Summary of Position Paper Approved by the ACP Board of Regents, July 2011

What is Health Information Technology?

Health Information Technology (HIT) is technology that enables health information to be collected, stored, and used electronically. The nature of HIT generates several kinds of important information, including individually identifiable health information (IIHI), which is any health data or record that could be correlated with a particular individual. IIHI that is transmitted by, or maintained in, electronic media or any other form or medium is considered to be protected health information (PHI).

How Does It Relate to Privacy?

As health care in the United States moves from paper to an increasingly electronic world, a new national debate over privacy of IIHI has emerged. Patients benefit when information pertinent to their care, concerns, and preferences is shared among those rendering health care services to them. However, patients need to feel confident that they can receive needed health care without the risk that their private information will be inappropriately disclosed, as such concerns might result in withholding of information and lead to potentially negative clinical consequences.

While many health policy experts and health care professionals anticipate improvements in clinical care and advances in research that could result from appropriate sharing of health information, a balance must be achieved between the need for complete, accurate, and available medical records and the requirement that all protected health information be secure and confidential to best serve the interests of the patient.

Key Findings and Recommendations from the Paper

ACP's recommendations center on the following key concerns:

- Preserving patient-clinician trust
- Addressing liability concerns among clinicians
- Defining and consistently applying an appropriate taxonomy (a set of terms that describe the range of privacy permissions) and framework
- Educating clinicians and patients about existing laws and regulations
- Protecting privacy

Specifically, ACP recommends the following:

- Privacy policies should accommodate patient preference so long as they do not negatively impact clinical care, public health, or safety.

- Under a revised privacy rule, permitted activities not requiring consent should include well-defined socially valuable activities involving public health reporting, population health management, quality measurement, education, and certain types of clinical research.
- Further, ACP supports protecting PHI and IIHI to the extent possible. Whenever a health care provider discloses PHI for a purpose other than for treatment, that disclosure should be limited to the minimum data necessary for the purpose based on the judgment of the provider.
- A revised privacy rule should maximize appropriate uses of information to achieve scientific advances without compromising ethical obligations to protect individual welfare and privacy. In addition, privacy laws and regulations must apply to all individuals, organizations, and other entities that have any contact with IIHI.
- There must be agreement on a basic privacy model and definitions, and there must be a single, comprehensive taxonomy for consent provisions and a standard structure for consent documents.
- Individuals should be able to access their health and medical data conveniently, reliably, and affordably, and should be able to review which entities and providers have accessed their IIHI.
- Patients should have specific, defined rights to request that their IIHI not be accessed through a health information exchange (HIE), a service that facilitates the exchange of patient information among physicians and other health professionals within a limited geographic area. Further, patients should have complete flexibility in making disclosure choices with regard to information stored in their personal health record (PHR), though any information that originated in a PHR or passed through a patient's control must indicate this fact as the information travels through the health care system.
- The nature of every agreement between entities that involves sharing of PHI should be made public.
- Enforcement of penalties for intentional or negligent breaches of privacy should be strictly enforced, and state attorneys general should be empowered to enforce privacy rules.
- New approaches to privacy measures should be tested before implementation.
- Use of a Voluntary Universal Unique Healthcare Identifier (an ID similar to a Social Security Number that would be assigned to a patient and used for all interactions with the healthcare system, but would not be used for any other purpose) could provide privacy benefits, and its potential use should be studied.

For More Information

This issue brief is a summary of *Health Information Technology & Privacy*. The full paper is available at http://www.acponline.org/advocacy/where_we_stand/policy/hit_privacy.pdf.

HEALTH INFORMATION TECHNOLOGY & PRIVACY

A Position Paper of the
American College of Physicians

This paper, written by Thomson M. Kuhn, MA, Michael S. Barr, MD, MBA, and Lois Snyder, JD, was developed for the Medical Informatics Subcommittee and the Medical Informatics Committee of the American College of Physicians (ACP) – 2008-2011; William R. Hersh, MD, (*Chair 2008-2009*), Mitchell A. Adler, MD, Abha Agrawal, MD, Sameer Badlani, MD, David W. Bates, MD, Robert Braham, MD, James J. Cimino, MD, Floyd P. Eisenberg, MD, Jeffrey P. Friedman, MD, Frederick S. Kelsey, MD, John R. Maese, MD, Nareesa A. Mohammed-Rajput,MD, J. Marc Overhage, MD, Daniel Z. Sands, MD, Paul Tang, MD, James M. Walker II, MD, (*Chair 2009-2011*), Alan H. Wynn, MD, and Michael H. Zaroukian, MD (*Chair 2011*); and for the Medical Service Committee – 2008-2009; Yul D. Ejnes, MD, (*Chair*), Mary M. Newman, MD (*Vice Chair*), Anne-Marie Audet, MD, Peter Basch, MD, Stephen D. Fihn, MD, MPH, Mandy Krauthamer, MD, Michael D. Leahy, MD, Keith Michl, MD, , Stephen G. Pauker, MD, Mark Richman, MD, Michael C. Sha, MD, and Rama Shankar, MBBS; and the Ethics, Professionalism and Human Rights Committee – (2010-2011); Kesavan Kutty, MD, (*Chair*), Joseph J. Fins, MD, (*Vice Chair*), Jeffrey T. Berger, MD, Clarence H. Braddock, III, MD, CPT. Tatjana P. Calvano, MC, USA, Kathy Faber-Langendoen, MD, Faith T. Fitzgerald, MD, Robert G. Luke, MD, Tanveer P. Mir, MD, Alejandro Moreno, MD, Amirala S. Pasha, J. Fred Ralston, Jr., MD, Michael C. Sha, MD, and Upasna Swift, MBBS.

It was originally approved by the ACP Board of Regents on 20 April 2009. This revised version was approved by the ACP Board of Regents on 30 July 2011.

HEALTH INFORMATION TECHNOLOGY & PRIVACY

Introduction

As U.S. health care moves from paper to an electronic world, a new national debate over privacy of individually identifiable health information (IIHI) has emerged. The patient-doctor relationship is dependent on trust—and this extends to the personal information shared as part of that relationship. Patients need to feel confident that they can receive needed health care without the risk that their private information will be inappropriately disclosed, which might result in withholding of information and lead to potentially negative clinical consequences. Patients benefit when information pertinent to their care, concerns, and preferences are shared among those rendering health care services to them.

Many health policy experts and health care professionals anticipate improvements in clinical care and advances in research that could result from appropriate sharing of health information. Individual patients will benefit when their providers are fully informed, and the public as a whole will benefit when patient data can be aggregated and studied. However, there is considerable tension between those who want to use the information for broader purposes (beyond that needed for patient care) and those who want to enable individuals to sequester all or part of their medical record due to the potential for inappropriate disclosure of this information. Some patients are genuinely concerned that well-meaning but insufficient attempts to keep information secure will ultimately fail and have a negative impact on individuals. News reports about disclosures of IIHI (both accidental and intentional) add to the momentum behind calls by some privacy advocates* for very stringent rules, regulations, and penalties for disclosure. Unfortunately, these fears have led to proposals for restrictions on necessary, beneficial, and timely uses of IIHI (see definitions below). For example, New York is contemplating a requirement for written patient consent from each provider group in order to access health information electronically with two choices: grant consent or deny consent. The unintended consequence of this proposed policy has been a subsequent interpretation that denying consent also bars access to the information in an emergency. A balance needs to be achieved between the need for complete, accurate, and available medical records and the requirement that all protected health information be secure and confidential to serve the best interests of the patient.

ACP strongly believes in the goal of widespread adoption and use of health information technology (HIT) to improve the quality of care. The College supports the concept of safe and secure electronic health information exchange (HIE) and advocates that clinical enterprises, entities, and clinicians wishing to share health information develop principles, procedures, and polices appropriate for the electronic exchange of information necessary to optimize patient care.

* Note that when privacy advocates are referenced in this paper, we are referring to some individuals and groups who have taken strong positions favoring privacy concerns over information sharing. Not all privacy advocates agree on all positions.

This policy paper attempts to describe the key issues and to provide recommendations to help achieve such a balance. Privacy policies need to satisfy the growing expectations that the implementation of computerized and networked medical records will facilitate better care at lower overall costs while preserving the expressed intent of the following principle from the Hippocratic Oath, “All that may come to my knowledge in the exercise of my profession or in daily commerce with men, which ought not to be spread abroad, I will keep secret and will never reveal.”

Definitions

Major sources of disagreement over privacy issues can sometimes be traced back to the use of different definitions for key terms. In this document, we define these key terms as follows (terms are ordered according to relationships with other terms):

Privacy—The right of patients for their personal information not to be divulged (disclosed) to others.

Confidentiality—The obligation of all holders of Individually Identifiable Health Information (IIHI) to protect the information according to the privacy interests of the patients to whom the information relates. A patient expects (trusts) that data that have been shared with a provider will not be further shared inappropriately.

Individually Identifiable Health Information—Any health data or record that could be correlated with a particular individual.

Protected Health Information—In this paper, refers to the specific meaning of the term as used in the current version of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule. PHI is IIHI that is transmitted by, or maintained in, electronic media or any other form or medium. If the information identifies or provides a reasonable basis to believe it can be used to identify an individual, it is considered IIHI. See Part II, 45 CFR 164.501.

Security—A patient expects all who hold IIHI (or PHI) to hold it securely. The patient expects that the holders will take all reasonable and appropriate measures to prevent the unintended disclosure of IIHI. Holding IIHI securely also involves protecting the information from inappropriate alteration and providing comprehensive auditing and logging of all actions taken that involve the IIHI.

Consent—Although not explicitly defined by HIPAA, "consent" is generally considered to mean written or verbal permission by an individual allowing others to use or disclose IIHI. Consent is related to, but not synonymous with, authorization. However, the term “consent” is used consistently in this document.

Treatment—The full range of direct patient care activities, including diagnosis and determination of prognosis.

Background

Patients are often surprised to learn the extent to which their PHI is shared under the current Federal HIPAA Privacy Rule and state-specific legislation. The complex nature of modern health care requires that many individuals and businesses other than their health care providers view PHI as part of routine operations (e.g., for coding, reimbursement, insurance claims). Beyond such uses for what are commonly called treatment, payment, and operations (TPO), PHI is used by researchers, public health organizations, advertisers, pharmaceutical companies, insurers, quality measurement organizations, and governmental agencies, among many others. Under some proposed forms of HIE, patient data may be stored in large regional repositories to make future access easier. The implication of this dispersion of PHI is that it is virtually impossible to report to patients every instance of access to their PHI with the detail that some privacy advocates have proposed.

In the United States, the HIPAA Privacy Rule was written in an attempt to minimize disclosure of PHI beyond what the rule considers to be legitimate uses (i.e., TPO). This rule currently sets the "floor" for privacy. Individual states are able to add further protections, and many have done so.

Table 1: Key Privacy Principles in HIPAA's Privacy Rule Principle

Parameter	Description
Uses and disclosures	Provides limits to the circumstances in which an individual's protected health information may be used or disclosed by covered entities and provides for accounting of certain disclosures; requires covered entities to make reasonable efforts to disclose or use only the minimum necessary information to accomplish the intended purpose for the uses, disclosures, or requests, with certain exceptions, such as for treatment or as required by law.
Notice	Requires most covered entities to provide a notice of their privacy practices, including how personal health information may be used and disclosed.
Access	Establishes individuals' right to review and obtain a copy of their protected health information held in a designated record set.
Security	Requires covered entities to safeguard protected health information from inappropriate use or disclosure.
Amendments	Gives individuals the right to request from covered entities changes to inaccurate or incomplete protected health information held in a designated record set.
Administrative requirements	Requires covered entities to analyze their own needs and implement solutions appropriate for their own environment based on a basic set of requirements for which they are accountable.
Authorization	Requires covered entities to obtain the individual's written authorization or consent for uses and disclosures of personal health information, with certain exceptions, such as for treatment, payment, and health care operations, or as required by law. Covered entities may choose to obtain the individual's consent to use or disclose protected health information to carry out treatment, payment, or health care operations but are not required to do so.

Source: GAO analysis of HIPAA Privacy Rule.

Recent Developments

Privacy advocates argue that the HIPAA Privacy Rule, especially if modified from its original form, is inadequate to meet patient privacy needs. (In 2002, HHS adopted modified guidance that relaxed consent requirements for certain operations.) They argue that TPO was redefined to include too many activities that should require consent. They also argue that the consent requirements are too vague and lax, reporting of disclosures is inadequate, and not every entity with access to PHI is covered by the rule. In addition, privacy advocates argue that emergence of HIEs and development of a National Health Information Network (NHIN) result in whole new classes of disclosure that are not addressed in current legislation and regulation.

At the state level, advocates have been successful in advocating for stricter laws and regulations regarding PHI protections and consent requirements. Unfortunately, this has resulted in a patchwork of sometimes conflicting rules, causing confusion, increased costs, additional barriers, and potential for errors among providers. For example, in Massachusetts, consent is required for any disclosure of mental health data, drug use history, history of sexually transmitted disease, and HIV status (except for public health reporting). In addition, such state-specific regulation complicates development of the appropriate interoperability standards and rules necessary to achieve the benefits of HIE. Creating a level of standardization would reduce the variability among state-specific policies, which even today further complicate electronic exchange of health information across geographic boundaries.

While there is growing concern among many in health care that attempts to protect privacy are overreaching and will have unintended negative consequences on advancement of HIT adoption and use, there are also those who want to use the transition to electronic records as a door to aggregating PHI for other purposes. For example, the California Integrated Healthcare Association will require doctors to disclose *all* patient laboratory test results to participate in the IHA pay-for-performance program or face a 75% decrease in the performance incentive (http://www.iha.org/p4py6.htm). Such "pay for data" initiatives place providers in the untenable position of potentially having to violate patient trust in exchange for payment.

Another significant development in the health care environment is the emergence of applications that allow patients to collect and manage their own IIHI. The emergence of Personal Health Records (PHRs) has fostered additional confusion over the fundamental nature and ownership of individual health-related information. There are many PHR-like applications available or under development, and there is no common agreement on what constitutes a PHR. Under the current HIPAA Privacy Rule, unless a PHR is provided by a health plan or other covered entity, the supplier of the PHR does not have to abide by the HIPAA regulations with regard to privacy. Further, the emergence of PHRs has resulted in new disputes regarding ownership, control, consent, attribution, sequestration, accuracy, and responsibilities for the data contained.

The recent and growing availability of personal genomic data poses new and complex privacy concerns. The emerging practice of personalized medicine involves the collection and maintenance of multigenerational data that, if disclosed inappropriately, could have devastating effects on the lives of those involved. The recently passed *Genetic Information Nondiscrimination Act (GINA)* offers some protection against inappropriate use of such data, but it cannot reverse the damage once a disclosure occurs.

Dimensions of Privacy

Protecting IIHI is far from simple–a broad range of issues must be addressed simultaneously. Attempts to tackle individual issues separately tend to fail and can have unintended consequences. Therefore, successful creation of policy that meets the needs of the current health care environment and minimizes unintended consequences must start with a comprehensive approach. This is a significant challenge because privacy requirements may vary based on several attributes, including but not limited to the following elements:

- Type of data (general health, mental health, HIV status)
- Purpose of use (treatment, payment, public health reporting, storage in a shared repository)
- Role of recipients (treating clinician, billing clerk)
- Individual recipient (a person performing an approved role but who has a personal relationship with the patient)
- Source of information (e.g., EHR, claims records, PHR , HIE, Regional Health Information Organization or RHIO)
- Patient characteristics (a minor; a particular diagnosis)
- Jurisdiction (local, state, and federal requirements may conflict).

Further, "consent" has many dimensions that need to be addressed in such a policy, including but not limited to:

- Patient factors—understanding, uncertainty, mental status, changing social, economic, or medical situation
- Format of consent (e.g., written, verbal)
- Situation (e.g., emergency, under duress, coerced)
- Medium (ink signature on form, note of verbal approval in chart)
- Time limits (expiration date, no expiration)
- Implied consent (opt-in, opt-out)
- How consent is documented
- How consent is communicated to health care providers
- How masking or sequestration of specific data is indicated or not indicated.

Policy Recommendations

The United States is slowly moving toward modernization of the health care system through the use of HIT. Unfortunately, we are faced with an unmanageable patchwork of laws and regulations regarding privacy and consent that is further complicated by new laws and regulations proposed in attempts to fix the holes in the patchwork. Absent a comprehensive approach, the U.S. faces the prospect of prolonged HIT gridlock as some privacy advocates promote tighter regulatory requirements in response to the perception that technology will eliminate existing protection and/or introduce new and more pervasive ways of breaching patient privacy.

Any changes in legislation must take into account the perspectives of all stakeholders, as the impact of modifying or replacing the existing definitions, structures, and interpretations of current law would have wide-ranging and dramatic consequences. The impact of policies adopted and implemented to address these complex concerns could be substantial with respect to the accuracy, reliability, usability of information exchanged electronically, and cost to implement. Such change cannot be accomplished by Congress, the Department of Health & Human Services, or the states acting alone. Further, the scope of such legislation would need to address the following key concerns:

- Patient–clinician trust. A balance must be achieved between the need for a complete, accurate, and available medical record and the requirement that all protected health information be secure and confidential and serve the best interests of the patient. Health care providers require all relevant and accurate information in order to provide the best possible care. Patients will only give full and accurate information if they are comfortable that this information will not be shared inappropriately. The interests of doctor and patient are closely aligned. Both will benefit to the extent that further disclosure of patient-supplied information is prevented.

- Liability. The confusing and overlapping laws and regulations surrounding patient privacy cause great concern to health care providers regarding their potential liability for noncompliance. Clinicians will err on the side of nondisclosure to minimize perceived risk. HIEs will only succeed if most providers participate. Concern over potential liability for improper downstream use of appropriately supplied PHI will reduce participation in the exchange and the likelihood of success.

- Taxonomy and framework. We cannot expect to achieve consistent application of privacy principles unless there is a defined and consistently applied taxonomy and framework for specification of privacy and consent.

- Education. Some controversy is based on misinformation and misunderstanding about existing laws and regulations and their application and limitations. These are complex problems that are poorly understood by most patients and health care providers.

- Erosion of privacy. Privacy is slipping away due to commercial interests, escalating reporting requirements (i.e., performance-based compensation arrangements), and efforts by insurers to collect more and more detailed information to support payment of claims.

Many organizations have given careful thought to the problem of privacy over the last few years. Appendix 1 is an annotated bibliography of some of the most important contributions to this literature. The publications of several of these organizations provide the foundation upon which we have built some of our policy positions. However, our position statements clearly diverge from several of these earlier works.

Our main conclusion is that the only solution to the current stalemate over privacy is for all stakeholders (including all classes of providers, governmental bodies, consumers, payers, quality organizations, researchers, and technologists) to work together to develop a comprehensive

framework for privacy and consent. This framework would clearly specify appropriate activities, such as treatment, payment, and some health care operations, where sharing of PHI can proceed without the need for additional consent. Once the boundaries of appropriate data sharing practices and situations are agreed on, it will be far easier to define the consent requirements for other activities that occur outside of the permitted zone.

Therefore, ACP proposes the following policy positions to guide the development of such a comprehensive framework:

Position 1: ACP believes that protection of confidential data is important for the safe delivery of health care. Privacy policies should accommodate patient preference/choice as long as those preferences/choices do not negatively impact clinical care, public health, or safety.

The College supports full disclosure of all relevant data to all treating clinicians. As a general rule, consent provisions should not apply to activities involving the sharing of IIHI among clinicians caring for a particular person. The potential risks and burdens of administering any consent provisions outweigh the risks of inappropriate disclosure in most cases. We recognize that under extreme circumstances full disclosure could negatively impact care delivery. For example, we support specific privacy protections for mental health therapy notes. However, we believe that certain other data types, such as medications, allergies, and results of laboratory testing and imaging procedures, should be represented because they are essential elements of the medical record and critical for effective clinical evaluation and safe therapeutic practices. The absence of such information—or even delayed access—could result in otherwise avoidable patient harm. Further, the source of all health information represented should be identifiable and an audit history of any changes made to this information needs to be available. Where state regulation or other policies dictate the protection of certain elements of the medical record so that they are not visible to an otherwise authenticated and authorized user, the record should specifically indicate the restricted nature of the missing data and provide a clear reason for the restriction (e.g., state law, mental health condition, and patient choice). Even with these indicators in place, we remain concerned about physicians' ability to fully trust a medical record when a patient, who generally is not a clinician, has chosen to restrict access to clinical information.

Position 2: ACP believes that under a revised privacy rule, permitted activities not requiring consent should include well-defined socially valuable activities involving public health reporting, population health management, quality measurement, education, and certain types of clinical research. Further, ACP supports the following principles on the use of Protected Health Information (PHI) and Individually Identifiable Health Information (IIHI):

A. **The sale of any IIHI without the patient's permission should be expressly prohibited.**
B. **Whenever possible and appropriate, de-identified, anonymized, or pseudonomized data should be used. The method used to remove identifiers should be publically disclosed.**

C. **IIHI should only be supplied in cases where such information is necessary for proper performance of a specific function. For example, if the goal is to count incidence of a disease or count the number of patients receiving an intervention, there is no need to include IIHI. Determination of the need for identifiable information should be made by appropriate publicly accountable decision-making bodies (e.g., Department of Health and Human Services, regional or local Institutional Review Boards [IRBs])**
D. **ACP recognizes that certain activities may not require individual authorization for the use of PHI and IIHI and recommends that whenever possible, all attempts should be made to de-identify PHI and IIHI in the context of educating current and future clinicians. Use of PHI and IIHI in educational and training activities, such as grand rounds and teaching conferences, should be minimized, although access to information in the clinical setting should be permitted as appropriate.**
E. **The public must be educated about the benefits to society that result from the availability of appropriately de-identified health information.**
F. **There should be tighter controls against improper re-identification of de-identified patient data.**
G. **Appropriately de-identified patient data should be available for socially important activities, such as population health efforts and retrospective research, with appropriate IRB approval and adherence to standards for de-identification. (See: *Standards for privacy of individually identifiable health information final rule. 67. Federal Register. 2002:53181–53273; Malin B, Benitez K, Masys D. Never too old for anonymity: a statistical standard for demographic data sharing via the HIPAA Privacy Rule. J AM Med Inform Assoc 2011;18:3-10.*)**
H. **ACP believes that information may be disclosed without authorization to public health authorities as required by law in order to prevent or control disease, injury, or disability.**

Position 3: ACP believes that whenever a health care provider discloses PHI for any purpose other than for treatment, that disclosure should be limited to the minimum data necessary for the purpose based on the judgment of the provider.

A. **While we agree conceptually that there could be benefits from application of "minimum necessary" criteria to activities involving payment and operations, current science and technology are not up to the task. It is not possible or appropriate to disentangle a clinical encounter note into relevant and nonrelevant elements.**
B. **As long as health plans require submission of complete notes from the patient record before approving payment, providers have no choice but to provide complete notes.**
C. **Health information technology (HIT) should incorporate audit trails to help detect inappropriate access to PHI.**
D. **Health care providers should be required to notify patients whenever their records are lost or used for an unauthorized purpose.**

E. Health care providers should not be penalized for failure to comply with requests for PHI that, in their judgment, are inappropriate under disclosure rules after notifying the requester that the request is being denied.
F. Health care providers should not be held responsible for actions taken by another entity with regard to PHI that the provider supplied to that entity in accordance with privacy regulations.

New Position 4: Regarding research, a revised privacy rule should maximize appropriate uses of information to achieve scientific advances without compromising ethical obligations to protect individual welfare and privacy.

A. Participation in prospective clinical research requires fully informed and transparent consent that discloses all potential uses of PHI and IIHI, and an explanation of any limitations on withdrawing consent for use of data, including biological materials.
B. ACP recognizes that further study is needed to resolve informed consent issues related to future research use of PHI and IIHI associated with existing data, including biologic materials.
- **Proposed informed consent models include: specific consent (reconsent required for new use of data); tiered or layered consent (menu of options to indicate whether reconsent is required); general permission or open-ended consent (all future uses permitted with IRB review); and blanket consent (no restrictions on future use). The 2009 Institute of Medicine (IOM) report, *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research*, recommends allowing future use of existing materials for research if the following conditions are met: "(1) the individual's authorization describes the types or categories of research that may be conducted with the PHI stored in the database or biobank; and (2) an IRB determines that the proposed new research is not incompatible with the initial consent and authorization, and poses no more than a minimal risk."**

C. Informed consent documents should clearly disclose whether law enforcement agencies would have access to biobank data without a warrant.
D. ACP recommends that regulations governing IRB review be expanded to include consideration of the preferences of research subjects whose tissue has been stored.

Position 5: ACP believes that privacy laws and regulations must apply to all individuals, organizations, and other entities that have any contact with IIHI.

A. Privacy protections that apply to all holders of IIHI, including services that store IIHI, should be addressed through new and comprehensive legislation.
B. The College supports approaches that ensure that all holders of IIHI are held appropriately accountable for their actions.

Position 6: ACP believes that there must be agreement on a basic privacy model and on definitions for all terms used. There must be a single, comprehensive taxonomy for consent provisions as well as a standard structure for consent documents. Therefore, ACP recommends that the National Committee on Vital and Health Statistics (NCVHS) convene an expert panel to address these issues.

A. **The privacy model must be unambiguous regarding which activities are permitted and which require consent.**
B. **Increasingly narrowly defined consent requirements cause unacceptable burdens on people and systems, and may increase health risks and legal liability. For example, rules that allow the withholding of consent for disclosure of individual prescriptions, laboratory results, or diagnoses pose unacceptable barriers to delivery of health care.**
C. **If consent is to operate effectively in a networked environment, the forms and content of consent artifacts must be at least as interoperable as the patient data to which they apply.**

Position 7: ACP agrees that individuals should be able to access their health and medical data conveniently, reliably, and affordably. Further, individuals should be able to review which entities and providers have accessed their IIHI and when access occurred according to the following principles:

A. **Full access to medical records and disclosure records will not be possible until electronic health record (EHR) systems and health information exchanges (HIEs) are capable of exchanging such information in electronic form. While we support patient rights to their information, we cannot support requirements to provide the information until systems are capable of providing it in a transparent, efficient manner.**
B. **Patients should have the right to request their information from every holder of information about them. Providers should be permitted a reasonable period to comply and to charge the patient a fee that is based on the cost of providing the information. Electronic medical records systems should be required to facilitate the provision of a patient's information in electronic formats. EHR and personal health record (PHR) vendors should be encouraged to ensure that their systems are interoperable.**
C. **Patients should have the right to request from any provider information about disclosures of their IIHI, other than disclosures made in the normal course of treatment, payment, and operations. Appropriate data would include the nature of the information, to whom it was disclosed, and when it was disclosed.**
D. **Electronic medical records systems should facilitate provision of information regarding all disclosures of patient data to users outside of the practice, other than disclosures made in the normal course of treatment, payment, and operations.**

It is important to note that attempts to impose new and cumbersome burdens on providers who choose to move from paper to computerized systems may backfire with serious negative consequences for societal attempts to improve health care with technology. As providers

examine the full range of additional obligations and liabilities that are being imposed on users of EHRs, many may find that the prudent course is to stay with paper-based practices. Legislators and regulators have an obligation to ensure that technology is implemented in ways that reduce burdens that hamper care delivery. HIT systems should be required to facilitate new administrative and reporting requirements that are imposed on providers. However, these requirements will probably result in increased costs and bloated systems, the costs for which will still fall upon the providers that the systems have, in theory, been designed to support.

Position 8: Patients should have specific, defined rights to request that their IIHI not be accessed through a health information exchange (HIE).

One model suggests that individuals control access by choosing either to have their entire record accessible through the HIE or not, rather than by selecting specific elements of the record for viewing. We acknowledge that this "all-in/all-out" system is unrealistic given existing state laws and policies regarding the need to accommodate individual wishes (e.g., Washington state) as well as regional efforts under way that already provide a significant level of choice—regardless of whether individuals have availed themselves of these options. Unfortunately, the existing and growing variations in policies concerning consent policies across HIEs open providers to unexpected liabilities. These, and other related concerns, may lead providers to avoid exchanging PHI across different jurisdictions.

As with consent in general, we are concerned that overly granular consent provisions will create undue burdens and risks. A commonly used example of granular consent would be a case where the patient withholds consent related to one problem (including any mentions of that problem in encounter notes) or mention of one medication in a medication history. The emphasis should be on protecting the data that are stored on, or pass through, the HIE from improper use rather than requiring all HIE participants to be aware of and comply with potentially detailed and changing consent restrictions of every patient.

Position 9: ACP believes that patients should have complete flexibility in making disclosure choices with regard to information stored in their PHR. However, any information that originated in a PHR or that passed through a patient's control must indicate this fact as the information travels through the health care system.

- **A. It is crucial for the safety and health of the patient, as well as for protecting the liability of a provider's actions, that the source of all data in a medical record be clearly identified and maintained as the information moves from system to system because of the risk that such data could be altered and therefore not retain its accuracy and/or relevance for clinical care decisions.**
- **B. It is equally important that the dates and times of all creation and modification activities associated with the data be maintained with the data.**
- **C. If at any time patient data, which may have originated in a provider's EHR, is supplied from a PHR or other external patient-controlled systems, this fact should be assigned to the data.**

Position 10: ACP believes that the nature of every agreement between entities that involves sharing of PHI should be made public.

Position 11: ACP believes that enforcement of penalties for intentional or negligent breaches of privacy should be strictly enforced and that state attorneys general should be empowered to enforce privacy rules.

A. **Recent calls for increased penalties fail to acknowledge the near-total lack of enforcement of existing penalties. See "Nationwide Review of the Centers for Medicare & Medicaid Services Health Insurance Portability and Accountability Act of 1996 Oversight [A-04-07~05064]" (http://www.oig.hhs.gov/oas/reports/region4/40705064.pdf).**
B. **It is critical that rules and enforcement efforts distinguish between inadvertent and intentional activities.**
C. **Breach rules must not hold any parties responsible for the actions of other parties over whom they do not have direct control.**

Position 12: ACP believes that new approaches to privacy measures should be tested before implementation.

A. **Once implemented, federal agencies and other stakeholders need to monitor the impact of new privacy measures, watch for unintended consequences, and adopt a flexible approach to implementation**.

Position 13: ACP believes that use of a Voluntary Universal Unique Healthcare Identifier could provide privacy benefits and that its potential use should be studied.

Accurate identification of patients and accurate association of patients with their data is a safety issue. What increased risk would this identifier present beyond the actual risks inherent in our current identification system? What benefits might it offer? A voluntary universal unique identifier for patients that has no other use beyond associating them with their health records might be less risky than using a set of demographic information that could have value beyond identification for health care purposes. We believe that this issue should not be dismissed without thorough evaluation of the potential risks and benefits. We call for the Secretary of Health and Human Services to initiate a thorough study of the risks and benefits of a voluntary universal unique patient identifier.

Summary

The ability of HIT and HIE to enhance the quality of care and the efficiency with which care is provided will greatly depend on trust. Individuals and their health care providers will need to trust that the information provided is complete and accurate and the best available representation of data for the purpose identified. Anything short of these objectives will undermine the efforts to use HIT to achieve the quality improvements and cost-savings many have projected. To facilitate this trust, we first need to address the significant gaps in the availability of standards, controlled terminology, and the reference model to support the desired privacy and confidentiality features of any new or revised regulation. Development and testing of the

standards recommended are essential before implementation. It is also important that we remain aware of emerging implications of improved access to health care information. This improved access may create new expectations of and responsibilities for physicians, researchers, and entities to be aware of including the potential to act upon information generated across any HIE platform. Therefore, the medical, legal, financial, and workflow implications—as well as the reimbursement requirements of such expectations and responsibilities—warrant significant discussion and exploration. These are all challenging issues. We need to resist the temptation to reproduce the inadequacies of our existing paper-based systems for the sake of expediency or to avoid complexities that can be overcome by good debate and sound policies.

APPENDIX 1

Perspectives

Over the past decade, a broad range of organizations have formally considered and commented upon health care privacy issues. Below are references to a selection of such activities that informed this paper.

eHealth Initiative

eHealth Initiative Blueprint: Building Consensus for Common Action (2007)
http://www.ehealthinitiative.org/blueprint/keyPrivacy.mspx
eHealth Initiative identified a set of basic principles that have been broadly endorsed and cited by others.

1. Transparency of privacy rules and information use.
2. Limitations on collection and use of information.
3. Individual control and view of data sharing.
4. Security requirements.
5. Audit and notification of breaches.
6. Rules for accountability and oversight.
7. Privacy concerns must be at the forefront in standards deliberations.

American Medical Informatics Association

Policies and Practices to Look for from Organizations that Collect Your Personal Health Information: A Consumer Checklist
2007
http://www.amia.org/files/draftconsumerchecklist.pdf
AMIA has published guidance concerning the terms that consumers should look for when examining an organization's privacy policies.

National Committee on Vital and Health Statistics

http://www.ncvhs.hhs.gov/080220lt.pdf

In a February 20, 2008, letter to the Secretary, NCVHS, reported on 4 years of deliberations regarding individual control of health information. In the letter, NCVHS makes recommendations concerning sequestration methods and categories, notice of sequestration, and access to sequestered information. It is clear that the complexities of the subject would make implementation in systems extremely difficult, and would result in new safety concerns.

Markle Foundation

The Connecting for Health Common Framework for Networked Personal Health Information 2008
http://www.connectingforhealth.org/phti/

This public–private collaborative proposed a comprehensive framework of practices that would ensure proper handling of IIHI as it flowed to and from PHRs and other personally controlled health care applications. The College endorsed this framework as providing an excellent starting point for consideration of specific regulatory and legislative proposals for privacy protection.

The framework does not address all of the concerns of providers regarding privacy; however, this was not its goal.

Center for Democracy and Technology
Rethinking the Role of Consent in Protecting Health Information Privacy
January 2009
http://www.cdt.org/healthprivacy/200910126Consent.pdf

This paper represents a migration in the thinking of this center on the fundamental issue of consent. Their position is that consent should not be required for more tightly defined treatment, payment, and health care operations. Starting from this position greatly simplifies many of the choices one must make in such areas as sequestration and notification. CDT also contends that efforts to expand the scope of consent may actually weaken privacy. As the scope of consent documents becomes broader and more complex, the likelihood that the consent is truly meaningful decreases.

General Accountability Office (GAO)
HHS Has Taken Important Steps to Address Privacy Principles and Challenges, Although More Work Remains
GAO-08-1138 September 17, 2008
http://www.gao.gov/products/GAO-08-1138

Quoting from the GAO report.
HHS's privacy approach does not include a defined process for assessing and prioritizing the many privacy-related initiatives to ensure that key privacy principles and challenges will be fully and adequately addressed. As a result, stakeholders may lack the overall policies and guidance needed to assist them in their efforts to ensure that privacy protection measures are consistently built into health IT programs and applications. Moreover, the department may miss an opportunity to establish the high degree of public confidence and trust needed to help ensure the success of a nationwide health information network.

Department of Health and Human Services
The Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information
December 2008
http://www.hhs.gov/healthit/privacy/framework.html

In December, 2008, HHS released a new privacy framework. Many have argued that it is not sufficiently more specific than the previous efforts criticized by the GAO above.