

# DRAFT -- for WORKGROUP REVIEW -- DRAFT

(date)

The Honorable Michael O. Leavitt  
Secretary  
U.S. Department of Health and Human Services  
200 Independence Avenue, S.W.  
Washington, D.C. 20201

Dear Secretary Leavitt:

The American Health Information Community (AHIC) members identified and prioritized several “breakthroughs:” health information technology applications that could produce specific tangible value to healthcare consumers. The AHIC Chronic Care Work Group’s breakthrough includes both broad and specific charges as follows:

- **Broad Charge for the Workgroup:** Make recommendations to the Community to deploy widely available, secure technology solutions for remote monitoring and assessment of patients and for communication between clinicians about patients.
- **Specific Charge for the Workgroup:** Make recommendations to the Community so that within one year, widespread use of secure messaging, as appropriate, is fostered as a means of communication between clinicians and patients about care delivery.

While concentrating on deployment of the specific charge, the Workgroup identified five significant issues which could either preclude or enable successful implementation of both charges. The Workgroup’s recommendations presented in this letter address these five issues:

- Reimbursement
- Medical Liability and Licensure
- Systems Supporting Patient-Clinician Secure Messaging
- Consumer and Clinician Access
- Patient Identification, Authentication and Security

## BACKGROUND & DISCUSSION

### Chronic Illness and Patient-Clinician Secure Messaging

Approximately 50-60 million Americans live stably with at least one chronic condition -- most have more than one. This 20% of the US population interprets care which is safe, effective, efficient, timely, patient-centered, and equitable (the aims of the Institute of Medicine) broadly -- given that most of the care management occurs outside of the professional setting. Patients with stable chronic conditions manage a good part of their care themselves while monitoring diets, controlling weight, checking blood sugars, adjusting blood thinners, titrating asthma medications, etc. This population, above and beyond almost any other, requires frequent and easy communication with their clinicians for guidance and timely decisions so that their chronic condition can be better and more tightly managed in their home, work, and school environments

## **DRAFT -- for WORKGROUP REVIEW -- DRAFT**

with minimal disruption. Further, as technology continues to find new and better ways to gather and transmit information through monitoring and communication devices, there will be even greater opportunity to meet patients' needs for care wherever and whenever they require the time and expertise of their physician or clinician.

Technology alone, however, will not lead to better care and outcomes. How it is adopted and used are critical components of success, as are the financial and social policies which either incent or disincent the adoption and use by both clinicians and consumers. The following recommendations which address technical, financial, and social barriers are specific to secure messaging between patients and their physicians and clinicians. They are, however, applicable to all types of telehealth communications.

### **Secure Messaging -- Definition and Common Functionalities**

Secure patient-clinician messaging refers to communications between patients and clinicians who have an explicit measure of responsibility for the patient's care. In addition to online consultation, secure messaging between patients and their clinicians may be used for:

- Requesting Prescription Refills
- Scheduling Appointments
- Requesting Referrals
- Receiving Routine Test Results
- Receiving Reminders & Instructions

Secure messaging may occur through a secure unique portal, may be part of a shared electronic health record system, may be accessed through a delivery system's architecture or may be part of encrypted attachments to traditional email. Independent of the vehicle, secure messaging is characterized by clear guidelines for use, published by the AMA and AMIA, and a clear methodology for assessing value developed by the IOM and the American Telehealth Association.

Adoption by the practicing clinical community has, however, been limited. The following recommendations address the major barriers.

## **RECOMMENDATIONS**

### **I. Reimbursement**

While up to 80% of chronic care management takes place out side of the practitioner's office, he/she is only reimbursed for time and expertise if the patient makes the effort to make and keep an appointment for an office visit. Explanations on how to best manage the changing patterns of atrial fibrillation, advice on how to modulate insulin in a brittle diabetic, monitoring of blood pressure and titrating its medications all require office visits in order for clinicians to be compensated, though much of this information and guidance could be provided through remote communication. Lack of reimbursement for clinician time and expertise rendered outside of the office setting is the major barrier to widespread adoption of the use of secure messaging between

## **DRAFT -- for WORKGROUP REVIEW -- DRAFT**

clinicians and their patients. In situations where lack of compensation is not a barrier (salaried clinicians or fee for service reimbursement) both a positive return on investment (ROI) and improved quality of care have been noted by the entity holding responsibility for the costs of care.)

There are, however, multiple methods of reimbursement. Fee for service payments, capitation, salary, bundling of services, and pay-for-performance have each been observed to produce different behaviors in practicing clinicians. In a system where any one clinician is subjected to multiple methodologies, he/she will determine which workflows and practice approaches are likely to produce the best return on their time and effort. As an example, it has been demonstrated that a clinician must be able to offer the ability to communicate via secure messaging with at least 20 to 30% of his/her patients before he/she finds it worthwhile to change office workflows and practices to maximize its effectiveness.

Lastly, reimbursement for virtually any service has attendant guidelines that should be clearly defined.

**Recommendation 1.0: HHS should develop and regularly update the evidence base for informed reimbursement policies with respect to secure messaging between clinicians and their patients. This should include monitoring and reporting the effect of secure messaging on cost, quality of care, patient and caregiver satisfaction, and medicolegal issues.**

**Recommendation 1.1: HHS should compile and assess the effect of various reimbursement methodologies for secure messaging on physician workflow in various care models, and report on best practices.**

**Recommendation 1.2: Public and private payers (including CMS) should contribute to the evidence for and information base on reimbursement strategies through direct reimbursement, pilot or demonstration studies, or coverage analysis for internet based patient/clinician encounters in accordance with guidelines developed by the American Medical Informatics Association, the American Medical Association, and the Massachusetts Health Data Consortium for structured secure messaging and include, but not be limited to, encounters that qualify under CPT code 074T.**

## **II. Medical Liability and Licensure**

Existing state licensing laws prohibit a practitioner licensed in one state from providing advice/care/education using a remote communication modality to any of his/her patients residing in another state. Licensing alternatives, such as licensure by reciprocity, for the purpose of permitting reimbursable secure messaging between patients and clinicians across state lines should be considered.

In addition to providing better care to patients with chronic illness, patient/clinician communication may be critical in the event of a man-made (anthrax) or natural (H5N1 influenza)

## **DRAFT -- for WORKGROUP REVIEW -- DRAFT**

bio-event. Immediate, secure communication will provide information that can affect diagnostic, therapeutic and isolation decisions to avoid further spread. State licensing laws should not prohibit our ability to diagnose and treat individuals who have been exposed to fast-spreading, possibly deadly, biological agents.

**Recommendation 2.0: HHS should convene the appropriate state agencies and professional societies to develop and adopt new licensing alternatives which will address the ability to provide electronic care delivery across state boundaries while still ensuring compatibility with individual state requirements.**

### **III. Standards for Systems Supporting Secure Patient-Clinician Messaging**

Secure technology solutions for communication about chronic care delivery between clinicians, and between clinicians and patients, and for remote monitoring and assessment of patients, must be based on standard transactions before they can be widely deployed as a means of chronic care improvement. The solution will only be effective if the clinical data can be appropriately shared between parties with legitimate needs for the data. Web portals currently offer feasible solutions for secure messaging among clinicians and patients, however, their effectiveness is limited by a lack of standardization and interoperability. Certification of secure message transactions and portals by a recognized certification body has the potential to encourage more widespread utilization.

**Recommendation 3.0: The Office of the National Coordinator for Health Information Technology (ONC) should direct the Health Information Technology Standards Panel (HITSP) to define standards for secure patient-clinician messaging transactions so that they may be interoperable with electronic health records.**

**Recommendation 3.1: ONC should direct the Certification Commission on HIT to establish certification criteria for system interoperability with patient-clinician secure messaging.**

### **IV. Consumer and Clinician Access**

The benefits of HIT, particularly transactional functions, are of recognized value to consumers. However, several studies have suggested that certain populations are less likely to access health information services electronically than others. A number of factors have been identified that may contribute to this disparate use. In order to minimize disparities in health care related to use of health information technology, it is necessary to identify and confirm barriers to use and strategies to assure that secure messaging can be a viable technology for all population groups.

Providers also have variable access to HIT, particularly in areas where broadband is not available.

**Recommendation 4.0: AHRQ should conduct a synthesis of current knowledge from existing studies of health information technology use by elderly, ill, and**

## **DRAFT -- for WORKGROUP REVIEW -- DRAFT**

**underserved populations including an analysis of barriers and drivers. The barrier and driver analysis should elucidate for which subpopulations barriers can be overcome and how.**

**Recommendation 4.1: HHS and the private sector should report on internet availability to providers across the country and report on a plan and timetable to make internet available uniformly.**

### **V. Privacy and Security**

Accurate, verifiable, unique patient identification and authentication is a foundational requirement both for supporting secure messages between patients and clinicians as well as incorporating the documents created into electronic health records, both those maintained by healthcare organizations as well as personal health records which may be maintained by patients. Methodology for identifying and authenticating patients must be constructed in such a way as to promote patient trust in the process, transparency in the use of information provided, and adequate patient control over who may or may not access this information. Ideally, patient identifying components and the method for cross-matching these components between systems should be standardized to facilitate matching patient identification across multiple systems, multiple provider environments and multiple healthcare sectors--as long as patients have a full understanding of the potential risks and benefits of this capability and voluntarily chose to allow this level of interoperability.

Authentication is the first step to enabling a patient, or their proxy, access to their health information electronically and having a high level of assurance that the sender of health information is in fact the authoritative source for the information. A secure portal rather than common e-mail facilitates the identification/authentication process, provides a more acceptable level of security, and creates opportunities for structured data entry not routinely available in common e-mail systems. The e-authentication industry is advanced and authentication is an existing technology that healthcare can leverage.

**Recommendation 5.0: A FACA compliant, consumer empowerment subgroup comprised of privacy and security experts from all Community Breakthrough Workgroups should report a set of recommendations to the Community by 9/30/06. The recommendations should be targeted to apply to each Workgroup's specific charge and should outline:**

- **Methods of patient identification;**
- **Methods for authentication;**
- **Mechanisms to ensure data integrity;**
- **Methods for controlling access to personal health information;**
- **Policies for breaches of personal health information confidentiality;**
- **Guidelines and processes to determine appropriate secondary uses of data; and**
- **A scope of work for a long term independent advisory body on privacy and security policies.**

**DRAFT -- for WORKGROUP REVIEW -- DRAFT**

These recommendations are supported by information obtained through research and testimony to the Chronic Care Workgroup. Supporting documentation is available in the accompanying Notebook for the May 16, 2006 meeting and is available on line at [www.hhs/healthit.gov](http://www.hhs/healthit.gov).

Thank you for giving us the opportunity to submit these recommendations. We look forward to discussing them with you and the members of the American Health Information Community.

Sincerely yours,

(signature)

Craig Barrett, Ph.D.  
Co-Chair, Chronic Care AHIC Workgroup

(signature)

Mark McClellan, M.D., Ph.D.  
Co-Chair, Chronic Care AHIC Workgroup