CHRONIC CARE WORKGROUP

Key Recommendations

Reimbursement (1)

HHS should develop the evidence base for informed reimbursement policies with respect to secure messaging between clinicians and their patients.

Reimbursement (2)

HHS should be charged to develop a description of reimbursement methods suitable for secure messaging. These methods would need to address the heterogeneity of practice setting from traditional fee for service to the variety of capitated systems (IPA and integrated staff models) as well as newer, innovative proposal like the American College of Physicians Advanced Medical Home. (Timeline - six months) To develop these descriptions, HHS should utilize the experience of existing secure messaging systems to learn different reimbursement strategies and to identify current best practices regarding existing specific and auditable guidelines for reimbursement of secure messaging. (Concurrent - six months)

Preliminary Discussion Questions

CMS WG members provided input after the last vetting process, which has been incorporated into the draft reimbursement recommendations.

- Does ***Reimbursement (2)*** now add clarity and specificity to ***Reimbursement (1)***?
- Can we make these one well-defined recommendation, understanding that multiple agencies within HHS could be involved?

SLIDE 1

CHRONIC CARE WORKGROUP

Key Recommendations

Reimbursement (3)

HHS should identify opportunities to leverage existing programs using secure messaging between clinicians and their patients to:

- **reflect the diversity of current physician practices**
- **reimburse only for internet based physician/patient encounters that qualify under CPT code 074T**
- **used in accordance with guidelines as developed by the American Medical Informatics Association, the American Medical Association and the Massachusetts Health Data Consortium for secure messaging**
- **coincide with existing or planned HHS demonstration programs designed to promote health IT adoption, consumer directed healthcare, and/or pay for performance efforts**

Preliminary Discussion Questions

CMS WG members provided input after the last vetting process, which has been incorporated into the draft reimbursement recommendations.

Since ONC cannot unilaterally develop reimbursement methods and CMS has multiple ongoing demonstration projects involving chronic care, does the current ***Reimbursement (3)*** address the Workgroup's thinking?

SLIDE 2

CHRONIC CARE WORKGROUP

Key Recommendations

Reimbursement (4)

HHS should monitor and report on ongoing electronic communication experiences in various practices and in pilot studies to determine the effects of online communications on cost, quality, especially for chronic disease outcomes, medical legal concerns and patient and caregiver satisfaction.

SLIDE 3

CHRONIC CARE WORKGROUP

Key Recommendations

Medical Liability and Licensure

Given that existing state licensing laws did not anticipate secure messaging as an integral part of the healthcare process, it is recommended that the Secretary of HHS working with such stakeholder groups as the National Governors' Association, the Federation of State Medical Boards, and the National Council of State Boards of Nursing, explore new licensing alternatives to address the ability to provide electronic care delivery across state boundaries while still ensuring compatibility with individual state requirements in terms of licensing fees, CME, etc. Some alternatives could include licensure by reciprocity, similar to what exists between states in Australia, or utilizing a model comparable to a driver's license in which if you have a valid license from one state you are permitted to drive in any other state. Key stakeholders to include in discussions might include the American Medical Association, the American Nurses Association, and the American Bar Association.

Preliminary Discussion Questions

Could we remove the rationale and examples from the Recommendation, and put them instead in the explanatory paragraphs?

SLIDE 4

CHRONIC CARE WORKGROUP

Key Recommendations

Consumer-Clinician Workflow

Enable clarity around intangible value to consumer and value in consumer-physician work-flow

- **AHRQ should investigate the impact of secure messaging on improved workflow by identifying successful patient care models that leverage secure messaging**
- **AHRQ should quantify and qualify intangible ROI, e.g., peace-of-mind, for patients within these usage models**

Preliminary Discussion Questions

1. Can we further clarify “intangible value” ?
2. Are we interested in factors that enhance optimized workflow in physician offices?
3. Are we interested in factors that enhance patient use of secure messaging with their clinicians?

SLIDE 5

CHRONIC CARE WORKGROUP

Key Recommendations

Standards for Embedding Secure Consumer-Clinician Messages into EHRs (1)

The Office of the National Coordinator for Health Information Technology (ONC) needs to ask the Health Information Technology Standards Panel (HITSP) to prioritize harmonization of standards relevant to secure messaging that could be used by the Certification Commission for Health Information Technology (CCHIT) in certification criteria for systems supporting secure messaging.

Standards for Embedding Secure Consumer-Clinician Messages into EHRs (2)

ONC needs to ask CCHIT to establish certification criteria for patient-physician secure messaging.

Preliminary Discussion Questions

Are these two separate recommendations, one, directing HITSP to endorse standards for interoperability of secure messaging with electronic health records, and the other, directing CCHIT to include these standards in its certification processes?

SLIDE 6

CHRONIC CARE WORKGROUP

Cross Cutting AHIC Workgroup Recommendations

Consumer Access & The Healthcare Digital Divide

AHRQ should conduct a synthesis of current knowledge from existing studies of computer use by elderly and 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 they can be overcome.

Preliminary Discussion Questions

Is it reasonable to table this recommendation until further research is conducted on multiple remote clinical technologies as part of the Broad Charge?

SLIDE 7

CHRONIC CARE WORKGROUP

Cross Cutting AHIC Workgroup Recommendations

Patient Identification and Authentication

HHS, HITSP and the private sector should set as their top priority the ability to match patient identification across multiple systems. This is the single most important first step for nationwide interoperability. The standard should be ubiquitous across all healthcare environments such as long term care, ambulatory, acute, chronic or generated from an individual. Additionally, the standard should be ubiquitous across all healthcare sectors such as payer, provider, individual.

Preliminary Discussion Questions

Is it reasonable to endorse the formation of a group to address issues that cut across all AHIC Workgroups on the topics of: patient identifier, linkage to patient-specific information, authentication and authorization; also policy and technical considerations?

SLIDE 8

CHRONIC CARE WORKGROUP

Cross Cutting AHIC Workgroup Recommendations

Patient Identification and Authentication

HHS, HITSP and the private sector should set as their second priority the requirement of initial in-person authentication as the requirement for e-authentication and the use of a secure messaging portal for actual exchange of information between patients and providers. The e-authentication industry is advanced and is an existing technology widely used in industry that healthcare can leverage. Because of the sensitivity of health information, authentication should be in-person. This recommendation is not focused on the technology of e-authentication; instead it is focused on the minimum requirement to obtaining e-authentication (i.e. digital certificate etc). 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.

Preliminary Discussion Questions

Is it reasonable to endorse the formation of a group to address issues that cut across all AHIC Workgroups on the topics of: patient identifier, linkage to patient-specific information, authentication and authorization; also policy and technical considerations?

SLIDE 9