Disease Management Technologies for Secure Communication

Clinical Problem	Solution	Lessons Learned
Communicating requests, clinical information, questions, etc. between care givers and patients	Secure Messaging	+ Enables asynchronous communication + Maintains audit trail of communication + Helps patients communicate personal health information
	Web based secure email	+ Can audit when message is read - Additional step required to read secure message, i.e. opening a URL from a regular email that takes user to a secure message web site. - Extra web servers add cost
	Desktop Clients & Plug-ins	- Difficult to set up and require storage of digital certificates
	Password based email	+ Easy to use - Requires secondary method to distribute passwords - Least secure and least amount of sender control
	Key Exchange w/Global Authentication	+ Least amount of effort for the receiver + Can be used to identify when a recipient has not read a message - Addition of Key server from hosting organization
	Telephony	+ Takes advantage of more ubiquitous technology
Any person-to-person communication.	Voice	+ Covers largest part of population. + Most familiar form factor + Nurse phone calls to patients in disease management programs have been very effective in maintaining patient behavior changes - No automated documentation of interaction - May need to make several attempts to connect with other party
Patient needs to provide caregivers with self-measured data.	IVR inbound (from patient)	+ Does not require internet or PC proficiency, + Enables asynchronous communication, + Provides accurate transcription of discrete information - Patient must remember PIN - Information transferred limited
Caregivers need to ensure the collection of patient self-measured data.	IVR outbound (to patient)	+ Can provide automated means of reminding patients to do certain tasks or to supply information + Can provide patient option to listen to educational stories (example from San Francisco General) - Ensuring the intended party is the one who answered the call requires verification
Provide daily biometric data information between the PCP and/or other clinicians/caregivers and the patient.	Remote Patient Monitoring	+ Security ensured by direct dial up and individual associations between in-home hub, patient, and backend management software. + Currently in use by disease management industry - Lack of interoperability standards across technology platforms
For communicating personal health information to clinicians.	Physical Transport	+ Helps patients maintain contents and control access to a Personal Health Record
	USB Flash drives	+ Most PCs have multiple USB ports

		+ Patient in control - Ability to transfer patient data from physician EMR to USB not always possible. - If no network back up of data, then hard to keep data synched between encounters with different providers - If lost or stolen, only secure if data is stored encrypted and with multiple identity validation controls
	Smart Cards	+ Can accommodate either data on board, or ID and access permission on board with the data residing in a central server. - The infrastructure for smart cards in the US needs to be built. Includes standards for data representation and availability of readers on most PCs
	Bar coded	+ Cost
	Magnetic stripe	+ Cost - Data can be lost if strip is damaged (scratching, magnets, other cards)
	RFID	+ Very reliable - Cost and availability of scanners
	Integrated EHR	+ Transfer clinical data across the continuum of care between providers and to and from a personal health record + Promotes full electronic exchange of information - Complete continuum of care is not computerized - Electronic sharing of patient consents requires separate document management component within or in addition to EHR - Will of caregivers to share information is not present, in part due to financial incentives.
	HL-7	+ Mature standard for transferring clinical information - Variability in section of HL-7 make it more difficult to interface between competing vendor systems
	CCR/CDA	+ Content standard for communicating key clinical summary information - Immature standard, still needs to gain acceptance - (CCR is an immature standard and is not yet in use. CDA is a mature standard but it is not yet widely used

Secure Communication Technologies in use for Disease Management

Telephone
The plain old telephone system is the most widely used technology for communication between stakeholders in disease management programs.

Voice
At the basic level the telephone is used for voice communication between patients and their caregivers. This is the most familiar and ubiquitous technology. The advantages of voice communication include ability to cover the largest population of the available technologies, is the most familiar form factor, and proven effective. Voice telephony has the disadvantages that documentation of conversation is not automated, and stakeholders may need to attempt calls several times to execute conversation.

Interactive Voice Response (IVR) Systems
Inbound IVR systems provide for ease and accessibility of voice telephony with advantages of enabling asynchronous communication and accurate automated documentation of data. Disadvantages include patients needing to remember a personal identification number and phone number. Also the amount of information that can be transferred is effectively limited. Examples of use include South Carolina Heart Center that uses an IVR for patients to call in weight, blood pressure and pulse information as well as answering yes/no type questions about their condition. IVR (when coupled with an ACD) can also be used to place outbound calls to either provide information or elicit information like done by the inbound IVR. This technology enables a care giver to provide automated reminders to patients, provide information, or request information. At San Francisco General Hospital they use an outbound IVR to request clinical data information like SCHC does, and also enables the patient to request educational stories. Disadvantages of outbound IVR is ensuring that the person who answers the phone is the intended party.

Secure Messaging
Electronic online messaging that provides for secure communication between a member of the care team and the patient. Secure messaging provides for asynchronous communication and an audit trail of all communication. There are different technologies to provide secure messaging. This technology is more complicated than telephony. Some technologies such as web-based secure email require additional steps from the user to get an email then navigate to a URL to read the actual message. Key exchange systems provide improved ease of use by senders and receiver, but require steps needed to register email addresses. Password protected email is not practical for communication among larger number of users as would be the case with a physician or disease management nurse and their patients because of the need for communicating passwords through another channel.

A barrier to secure messaging is the need for personal computers and Internet access. There is added expense to maintain the password or keys.

Telemedicine (use of devices in home or Remote Patient Monitoring RPM))
Can use technology from POTS to broadband. Devices in the home are used to transmit information to the caregiver. Devices can range from simple scales, blood pressure cuffs, and glucometers, to systems that incorporate video cameras to enable more advance communication.

Remote patient (or physiologic) monitoring through an in-home hub communicating to some dedicated devices such as scales and blood pressure cuffs is in common use today by disease management companies. The devices are used to try and reduce telephone interactions, while still achieving the behavior modification outcomes.

A system is in use as part of a pilot at SUNY and Columbia University that incorporates blood pressure cuffs, glucometers and a video camera. Patients can enter their clinical information automatically and allows a nurse to check insulin draws before injection. Detroit Medical Center uses a system that has a box in the patient home that records blood pressure, pulse and weight and answers to some questions presented to the patient, this recorded data is then sent over the phone lines to the care giver. Other systems are becoming available that add additional functions and full video conferencing but require specific broadband carrier connectivity.

A barrier to wide spread use of these technologies is the need for specialized hardware, and in some situations specialized broadband connectivity. Physicians fear a loss of control in patient management.

Personal Health Records

Portable patient control health records are starting to gain use. Several models exist on how to securely move information between patients and care givers. Server stored systems enable password controlled access through secure messaging technologies. There are other models that use a smart card of USB flash drive key as a secure means of physically transporting the information between patient and provider.

Integrated Electronic Health Records

Systems like Kaiser are providing completely integrated EHRs. Theses systems provide secure access to the EHR through passwords (and possibly biometrics). This enables clinicians to access a patients complete clinical record. Extensions of this system enable a patient (and their caregivers) to see portions of their record and add to the record as part of a PHR. The data is an integral part of the EHR so the clinicians involved in care can see the PHR information as well. Since the data fully resides within the EHR there is less use of more global secure communication technologies. The system then provides abilities to escalate reminders to missing tasks to ensure patient/provider compliance with best practices. The other technologies that enable secure email or web services are available for transferring copies of data or reports to external parties (i.e. outside the patient and care team) through the other secure messaging technologies reported above.

Barriers to secure communication

Biggest barrier is the incentives to communicate at all. There are no incentives for the physician to share data with other providers. There is also concern in engaging in electronic communication with patients that it will increase workload without commensurate revenue.

Today's communication flows

Family to patient: This is usually a very strong channel but not well documented
Patient to clinician: This is usually a very strong channel, but not continuous and often relies on patient memory to provide much of the information
Patient to Disease Manager: This is usually a very strong channel; information is collected closer to time of occurrence
Disease Manager to primary clinician: This communication channel is often then weakest connection; much of the information sharing is done via letters or through the patient.

2/22/2006