**U.S. Department of Health and Human Services**

**Office of the National Coordinator for Health Information Technology**


# Patient – Provider Secure Messaging

# Detailed Use Case

# March 21, 2008

# Table of Contents

# List of Figures

# 1.0 Preface

Use cases developed for the American Health Information Community (AHIC) are based on the priorities expressed by the AHIC, which include needs expressed by the AHIC Workgroups. These high-level use cases focus on the needs of many individuals, organizations, and systems rather than the development of a specific software system. The use cases describe involved stakeholders, information flows, issues, and system needs that apply to the multiple participants in these arenas.

The use cases strive to provide enough detail and context for standards harmonization, certification considerations, architecture specifications, and detailed policy discussions to advance the national health information technology (HIT) agenda. These high-level use cases focus, to a significant degree, on the exchange of information between organizations and systems rather than the internal activities of a particular organization or system.

During the January 2007 AHIC meeting, nine priority areas (representing over 200 identified AHIC and AHIC workgroup detailed issues and needs) were discussed and considered. Three of these areas (Consumer Access to Clinical Information, Medication Management, and Quality) were selected for use case development and the final 2007 Detailed Use Cases were published in June, 2007.

The remaining six priority areas from the January 2007 AHIC meeting (Remote Monitoring, Patient-Provider Secure Messaging, Personalized Healthcare, Consultations & Transfers of Care, Public Health Case Reporting, and Immunizations & Response Management) have been developed as the 2008 Use Cases which will be processed in the national HIT agenda activities in 2008.

The 2008 Use Cases have been developed by the Office of the National Coordinator for Health Information Technology (ONC) with previous opportunities for review and feedback by interested stakeholders within both the private and public sectors. To facilitate this process, the use cases have been developed in two stages:

- The **Prototype Use Case** describes the candidate workflows for the use case at a high level, and facilitates initial discussion with stakeholders; and
- The **Detailed Use Case** documents all of the events and actions within the use case at a detailed level.

This document is the Detailed Use Case. Feedback received on the Draft Detailed Use Case has been considered and incorporated where applicable into this document.

This Detailed Use Case is divided into the following sections:

- Section 2.0, Introduction and Scope, describes the priority needs identified by one or more AHIC workgroups and includes draft decisions made regarding the scope of the use case.
- Section 3.0, Use Case Stakeholders, describes individuals and organizations that participate in activities related to the use case and its components.
- Section 4.0, Issues and Obstacles, describes issues or obstacles which may need to be resolved in order to achieve the capabilities described in the use case.
- Section 5.0, Use Case Perspectives, describes how the use case combines similar roles (or actors) to describe their common needs and activities. The roles are intended to describe functional roles rather than organizations or physical entities.
- Section 6.0, Use Case Scenarios, describes how various perspectives interact and exchange information within the context of a workflow. Use case scenarios provide a context for understanding information needs and are not meant to be prescriptive.
- Sections 7.0 and 8.0 provide a greater level of detail for each scenario and include information flows. Specific events and actions for each perspective and scenario are presented and discussed. These are also not intended to be prescriptive.
- Section 9.0, Information Exchange, describes the role of information exchange in the use case at a high level.
- Section 10.0, Dataset Considerations, identifies specific information opportunities relevant to this use case that may support future standardization and harmonization activities.
- Appendix A, the Glossary, provides draft descriptions of key concepts and terms contained in the detailed use case.

## 2.0 Introduction and Scope

In January 2007, the AHIC approved a recommendation to develop a use case addressing processes and information needs associated with patient – provider secure messaging. This use case discusses scenarios in which patients interact with their healthcare clinicians remotely using common computer technologies readily available in homes and other settings.

The broad term "patient – provider secure messaging" includes both secure messages sent from patients to providers as well as secure messages sent from providers to patients. Similarly, the use of the term "provider" includes clinicians and clinician support staff. Since "provider" is also occasionally used in the healthcare industry to indicate a more generic service or capability provider, the term "clinician" will be used more extensively in this use case to promote clarity.

Enhanced patient-clinician communications and effective management of chronic care conditions could be promoted by this form of electronic interaction. Communication could occur in a number of ways, but the most common would be through secure messaging. This messaging is similar to traditional email where both patients and clinicians can send and respond to communications without having to be on-line at the same time. This type of communication, frequently done with secure web technologies, is also known as asynchronous, "store and forward" communications.

In addition to patients and clinicians, communications could also include caregivers, family members, and patient advocates to further promote and coordinate patient care. Patients could also benefit from message-based prompts and reminders initiated by clinicians and their staff to remind patients and their advocates of recommended events and activities that are important to maintaining and improving health. Personal health information related to these prompts and reminders would need to be provided using messages that are communicated in a secure sending and receiving environment, also known as a secure communication channel. In specific terms:

- Giving patients the ability to compose and send a secure communication to a clinician will, at times, give them access to their clinicians in a more timely, efficient manner than an office visit or a phone call.

- Similarly, clinicians will benefit from having the ability to respond to or initiate secure communications to facilitate the care process and promote better patient health. This communication will be done in a manner which provides appropriate information to the patient and meets existing needs for clinical documentation.

- Giving clinicians the ability to securely communicate reminders to patients and their family members will promote preventive healthcare. These reminders could include

items such as annual check-ups, cancer screenings (e.g., mammograms and colonoscopies), and immunizations.

The scope of this use case excludes “live” (synchronous, real-time) communications via video links, text chat, and other technologies. This restriction provides focus to the use case on rapid implementation of interoperability and standards for the secure messaging capabilities described above.

Similarly, the use case is focused on patient – provider communications. Provider – Provider communications are included in the scope of the 2008 Consultations & Transfers of Care Detailed Use Case. Additionally, this use case is supportive of the interoperability and standards work related to the 2008 Remote Monitoring Detailed Use Case.

When describing secure messaging, the content of messages includes information specific to a particular patient – clinician transaction. These transactions and their information content may also be made available to patients through the use of secure internet web page access (e.g., “patient portals”). Moreover, secure messages may include message content as well as an implied process (e.g., pharmacy refill request). Therefore, these patient portal transactions accomplish secure information exchange and are within the target scope of this use case.

Similarly, messages can include structured and unstructured content, or a combination of the two. Certain content such as adult patient age is amenable to a structure that would restrict input to a whole number of years. Other content (e.g., patient’s chief complaint) might be better served through unstructured text. Likewise, structuring methods (e.g., the use of drop-down boxes or other familiar web-based presentation techniques) may be relevant for this discussion. Similarly, “secure forms” are another tool that can provide structured support for this information exchange and would be within the scope of this use case. This use case does not attempt to prescribe the use of structured or unstructured content for any particular type of message transaction. However, Section 10.0 – Dataset Considerations offers some initial ideas in this area.

One of the goals of the AHIC is establishing a pathway, based on common data standards, to facilitate the use of interoperable, clinically useful secure messaging information as a complement to, or as part of, electronic health records (EHRs) to support care, clinical decision-making and promote wellness and patient empowerment. This use case was developed to support the many stakeholders who are active in the development and implementation of Personal Health Records (PHRs), EHRs, and health information exchange capabilities including those engaged in activities related to standards, interoperability, harmonization, architecture, policy development, and certification.

The 2008 Patient – Provider Secure Messaging Detailed Use Case is based on the previously released Remote Consultation Prototype Use Case and focuses on the exchange of secure messages in two scenarios:

- **Patient-to-Clinician Communication.** This scenario is focused on the patient's ability to use computerized technologies that are readily available, such as secure web access, to communicate with clinicians using unstructured and structured messaging capabilities.

- **Clinician-to-Patient Communication.** This scenario includes the ability of clinicians to initiate communications to the patient and respond to their communications. This scenario also includes the ability of a clinician to send relevant clinical reminders to patients regarding medical screening examinations, regular diagnostic tests, or wellness activities.

# 3.0 Use Case Stakeholders

**Figure 3-1. Patient – Provider Secure Messaging Use Case Stakeholders Table**

| Stakeholder | Contextual Description |
|---|---|
| **Clinical Knowledge and Tool Suppliers** | Organizations that provide knowledge and tools to aid in the understanding and treatment of health and disease conditions. These tools may include knowledge regarding items such as clinical reminders, decision support, expertise, and research findings. The tools encompass a wide range of capabilities that may be useful and available to patients, consumers, clinicians, and other health professionals. These tools can also support secure messaging, educational materials, and messaging content. These suppliers may include developers, providers, resellers, operators, and others who may provide these or similar capabilities. |
| **Clinical Support Staff** | Individuals who support the workflow of clinicians. For this use case, this may be by receiving and evaluating communications from consumers or patients, and then engaging the appropriate clinician in the response to the patient. |
| **Clinicians** | Healthcare providers with patient care responsibilities, including physicians, advanced practice nurses, physician assistants, nurses, psychologists, pharmacists, and other licensed and credentialed personnel involved in treating patients. |
| **Consumers** | Members of the public that include patients as well as caregivers, patient advocates, surrogates, family members, and other parties who may be acting for, or in support of, a patient receiving or potentially receiving healthcare services. |
| **Electronic Health Record (EHR) / Personal Health Record (PHR) System Suppliers** | Organizations which provide specific EHR and PHR solutions to clinicians and patients such as software applications and software services. These suppliers may include developers, providers, resellers, operators, and others who may provide these or similar capabilities. |
| **Healthcare Entities** | Organizations that are engaged in or support the delivery of healthcare. These organizations could include hospitals, ambulatory clinics, long-term care facilities, community-based healthcare organizations, employers/occupational health programs, school health programs, dental clinics, psychology clinics, care delivery organizations, pharmacies, home health agencies, hospice care providers, and other healthcare facilities. |

| Stakeholder | Contextual Description |
|---|---|
| **Healthcare Payors** | Insurers, including health plans, self-insured employer plans, and third party administrators, providing healthcare benefits to enrolled members and reimbursing provider organizations. |
| **Patients** | Members of the public who receive healthcare services. |

## 4.0 Issues and Obstacles

Realizing the full benefits of HIT is dependent on overcoming a number of issues and obstacles in today's environment. Inherent is the premise that some of these issues and obstacles will be cross-cutting and therefore shown in all use cases, while others are unique to this specific use case. Some of these topics will appear in both the cross-cutting and use case-specific sections so that, in addition to the shared characteristics of the issue, considerations specific to a use case may be addressed.

Issues and Obstacles which are applicable across use cases appear below in problem and consequence form:

- **Confidentiality, privacy, and security:**
    - In order for consumers to accept electronic health records, appropriate privacy and security protections may be needed to manage access to personal health information. Consumers may also want to decide who will view and communicate their personal health information. Privacy and security controls and the means of restricting data access are not standardized or regulated.
        - Without permissions and controls, consumer participation in the act of electronic health information exchange may be limited.
    - There are regulations concerning the storage, transmission, or destruction of electronic health information. These regulations are inconsistent across federal, state, and local jurisdictions.
        - Without consistent standards, the viewing, accessing, or transmitting of electronic health information may be inhibited.
- **Information integrity, interoperability, and exchange:**
    - Incomplete, inaccurate, or proprietarily-formatted information prevents efficient health information exchange activities or utilization of electronic health information.
        - Without data standards that promote compatibility and interoperability, longitudinal patient medical records may be incomplete or of questionable integrity.
- **EHR and HIT adoption:**
    - The processes identified in the use cases rely upon successful integration of EHRs into clinical activities. Because this integration may not align with

current workflow and may require additional upfront costs, it may not be widely pursued or implemented.

- Low adoption of HIT, particularly within rural areas and long-term care settings, may create disparate service levels and may adversely affect healthcare for these populations.

- **Lack of business model and infrastructure:**
  - Financial incentives are not currently sufficient to promote the business practices necessary for sustainable HIT.
    - If sufficient reimbursement policies and other financial incentives are not established, HIT adoption may be difficult or unsustainable.
  - Activities involving health information exchange will require additional technical infrastructure, functionality, and robustness, beyond what is currently available.
    - Unless the requisite infrastructure for health information exchange capabilities is established, improved upon, and sustained, these capabilities may have limited success and provide few benefits.
- **Clinical Decision Support:**
  - The capabilities, requirements, and standards needed for consistent development, implementation and maintenance of Clinical Decision Support have not been identified.
    - The utility and benefits of Clinical Decision Support cannot be fully realized without the development of workflows and standards demonstrating benefits for consumers, patients, and clinicians.

In addition to the cross-cutting issues and obstacles described above, several other issues or obstacles exist that are specific to this use case.

- **Lack of business model and infrastructure:**
  - Expenditures for clinicians to implement secure messaging may not be reimbursable.
    - If reimbursement policies and other financial incentives are not established for IT investments, secure messaging may not be widely realized.

- Clinicians may not be paid, may only partially be paid, or may be paid only under certain circumstances for time spent on behalf of patients during secure messaging.
    - If reimbursement policies and other financial incentives are not established for time spent on secure messaging, this capability may not be widely implemented.

- **Confidentiality, privacy, and security:**
    - Secure messaging tools should address security needs in the disposition of all patient and clinician communications. Patient and clinician identities should be established to support non-repudiation of messages. Use of standard electronic mail is not considered adequately secure, and users of electronic mail should consider not include personal health data in this type of communication. Appropriate use of secured and unsecured messaging may not be understood by all parties engaged in secure messaging.
        - If secure messaging is not adequately implemented and understood, patient privacy needs may not be met.

- **Legal medical record:**
    - The potential impact of secure messaging on malpractice and malpractice insurance has not been established.
        - If malpractice risks related to the use of secure messaging are too great or not well understood, then widespread implementation and use of this patient-clinician communication will be lessened.
    - There is a lack of clarity about the scope of the legal medical record, particularly as it relates to secure messages sent between patients and their clinicians.
        - If a clear understanding of the appropriate treatment of secure messages with respect to the medical record is not established, implementation and use of secure messaging will be difficult.

- **Communication technologies:**
    - For secure messaging, appropriate messaging attributes and standards (such as sender verification, recipient verification, guaranteed delivery, and message acknowledgment) as well as those for security do not exist and must be identified.

        - If secure messaging standards and attributes are not established, an integrated, seamless secure messaging capability will be difficult.

    - Appropriate capture and archiving of secure messages within EHRs is not standardized.

        - If secure messaging interactions with EHRs are not standardized, EHRs with messaging content may be incomplete or difficult to use.

- **Secure messaging tool suppliers, users, and implementation practices:**

    - There are not consistent, standardized requirements for secure messaging capabilities, and information about how messages will be handled and users' rights may not always be transparent to users. Example capabilities that may not be clear to consumers are: 1) use of clinician support staff to access, read, preview, and process messages intended for clinicians; 2) clear indication on communications as to who is the actual message author; 3) potential access to consumer messages by non-provider entities such as payors, public health, or law enforcement; and 4) inclusion of support for a "For clinician eyes only" indication on messages containing very sensitive patient information.

        - If secure messaging capabilities are not understood by consumers, secure messaging use may be limited.

- **Information integrity, interoperability, and exchange:**

    - The quality of patient data will impact the appropriateness of reminders for patients. These reminders are dependent on accurate, reliable, and up-to-date medical history, some of which may be patient-entered, to alert patients about the appropriate steps to take for disease prevention and/or management. This level of accuracy may not be present in many medical histories today.

        - If medical histories are not sufficiently accurate, inappropriate reminders may be communicated.

    - Standards for the information which should be included in a patient reminder do not currently exist. A reminder that does not contain sufficient or correct information for the patient to act upon it may be confusing.

        - If reminder content is insufficient or inaccurate, appropriate action can not be taken by the patient.

# 5.0 Use Case Perspectives

The Patient – Provider Secure Messaging Detailed Use Case focuses on the ability of patients to interact with their healthcare clinicians remotely using computer technologies readily available in homes and other settings. Similarly, clinicians can use this capability to interact with their patients. The use case describes secure messaging from three perspectives. The perspectives are representative of roles and functions, rather than organizations or physical locations. The functions of clinical support staff in particular could be conducted by clinicians themselves. Each perspective is described below:

- **Patient**

  The patient (or consumer), caregivers, patient advocates or surrogates, family members, and other parties who may be acting for, or in support of, a patient could use secure messaging capabilities to interact with clinicians. This function or role initiates messages and responds to clinician messages as necessary to facilitate the patient healthcare process. The role of patient can include:

  - Patients;
  - Caregivers;
  - Patient advocates;
  - Surrogates;
  - Family members; and
  - Other parties who may be acting for, or in support of, a patient receiving or potentially receiving healthcare services.

- **Clinician**

  Clinicians may receive and respond to secure messages from their patients/consumers. Clinicians, or their EHR systems, may also initiate clinical reminders and similar messages for patients. This function or role conducts these activities to facilitate the patient healthcare process. The role of clinician can include:

  - Physicians;
  - Advanced practice nurses;
  - Physician assistants;
  - Nurses;
  - Psychologists;
  - Pharmacists; and
  - Other licensed and credentialed personnel involved in treating patients.

- **Clinician Support**

  The clinician support perspective includes those roles which support the workflow of clinicians by receiving and evaluating communications from consumers or patients, and then engaging the appropriate clinician to address the patient communication. These individuals may also support clinicians by coordinating communications and other care activities with patients on behalf of clinicians. The role of clinician support can include all of the personnel listed above in the clinician perspective but is likely focused on those who are supporting clinician workflow.

These perspectives are the focus of the events detailed in the scenarios described in Section 6.0.

# 6.0 Use Case Scenarios

The Patient – Provider Secure Messaging Detailed Use Case focuses on the ability of patients to remotely interact with their healthcare clinicians using computer technologies readily available in homes and other settings. Similarly, a clinician's ability to initiate communications to a patient (and respond to their communications) is also a focus for this use case. Patient caregivers, family members, and advocates may be included in these communications. Finally, clinical reminders sent from clinicians, or EHRs, to patients are included in these scenarios.

- **Patient-Initiated Communication**

  This scenario is focused on the patient's ability to use readily available computerized technologies to communicate with clinicians using secure messaging capabilities.

  - The patient initiates a message using a secure web browser, PHR, patient portal, or other messaging tool. Structured templates could be used to gather the needed clinical and administrative information from the patient including items such as patient identifying information, questions the patient would like to ask, or description of symptoms or problems the patient wishes to communicate to the clinician. Structured communications support efficient information exchange and clinician workflow. In addition, unstructured text must also be accommodated.

  - Patient communications could include communications related to patient self-monitoring or chronic care as described separately in the 2008 Remote Monitoring Detailed Use Case or the 2008 Consultations and Transfers of Care Detailed Use Case. Although most of that communication is intended to be from devices described in that use case, there may be instances where manually-gathered information is communicated via secure messaging. In addition, there may be communications between patient and clinician related to questions about device measurement data, supplemental patient health status information, treatments (or changes in treatments), or other care interactions.

  - The clinical support staff receives and evaluates the information supplied by the patient and either:

    - Responds directly to the patient and documents the communication event. This response may be discussed with the clinician. The response could occur in several ways, including such methods as a telephone call or unsecured message (e.g., email) advising the patient that a secure message is available to them containing sensitive clinical

information. It should be emphasized that secure messaging is not intended for use in emergency situations. If a patient communication indicates a need for emergency care or another medical intervention, the clinician should always be notified; or

- Forwards the information along with other relevant clinical information to the clinician for a response. This could be accomplished using the workflow capabilities of the clinician's EHR.

o Clinician responds to the patient after evaluating the patient's concerns and questions either directly to the patient or through the clinical support staff.

- Direct communication with the patient could occur in several ways such as a direct response in the secure messaging system, a telephone call or an email advising the patient that a secure message is available for them.

- Communication through the clinical support staff could be accomplished by using the workflow capabilities of the clinician's EHR, or through another mechanism. This communication could include instructions to be given to the patient, clinical care instructions or orders, or requests for additional information.

o At the conclusion of the communication exchange, the patient, the clinical support staff, and the clinician need to complete additional activities as necessary. This may be supported by automated tools that archive messages and associate them with patient medical records.

- **Clinician-Initiated Communication**

This scenario is focused on the clinician's ability to use secure messaging capabilities to communicate with a patient. This scenario includes the use of clinical reminders as communications from clinicians to patients regarding items such as medical screening examinations, regular diagnostic tests, or wellness activities.

o The clinician initiates a message using an EHR or other secure messaging tool. Structured templates could be used to request needed clinical and administrative information from the patient including items such as patient identifying information, questions the clinician may like to ask, or information related to a patient symptom or problem that the clinician wishes to communicate to the patient. These communications could also include follow-up to a previous visit, test, or lab result. Structured communications support efficient information exchange and clinician workflow. However, unstructured text must also be accommodated.

- Similarly, the clinician may use this secure messaging capability to respond to patient communications. As described above, the clinician may also rely on clinical support staff to support this capability on behalf of a clinician.

- Communications may include copied text or web links to other information that could promote patient understanding of medical conditions and patient/clinician working relationships.

- Communications between clinicians and patients could also include additional patient-related representatives such as care coordinators, caregivers, family members, and patient surrogates. Inclusion of these additional parties would be done in accordance with the patient's confidentiality and privacy preferences.

- Clinical reminders can be initiated by a clinician. These reminders can also be triggered by automated functions within an EHR that evaluate patient-specific information to determine the need for a reminder based on EHR data, best practices, and evidence-based guidelines. Reminders could include annual medical checkups, medical screening examinations, immunizations, or periodic requests for clinical information from the patient. Use of reminders by a clinician could be coordinated with appropriate eligibility and benefits considerations.

- Reminders could be delivered to the patient as:

    - Electronic mail informing the patient to retrieve a secure message (that may contain sensitive clinical information); or

    - Messages received by the patient's PHR or other secure messaging tool.

- Duplicate reminders could be sent to caregivers (e.g., family member, home health nurse, or care coordinator), based on automatic message routing and pre-established patient preferences.

- At the conclusion of the communication exchange, the patient, the clinical support staff, and the clinician complete information related to the communication event and perform documentation of the event as required. This may be supported by automated tools that archive messages and associate them with patient medical records.

# 7.0 Scenario 1: Patient-Initiated Communication

**Figure 7-1. Patient-Initiated Communication**

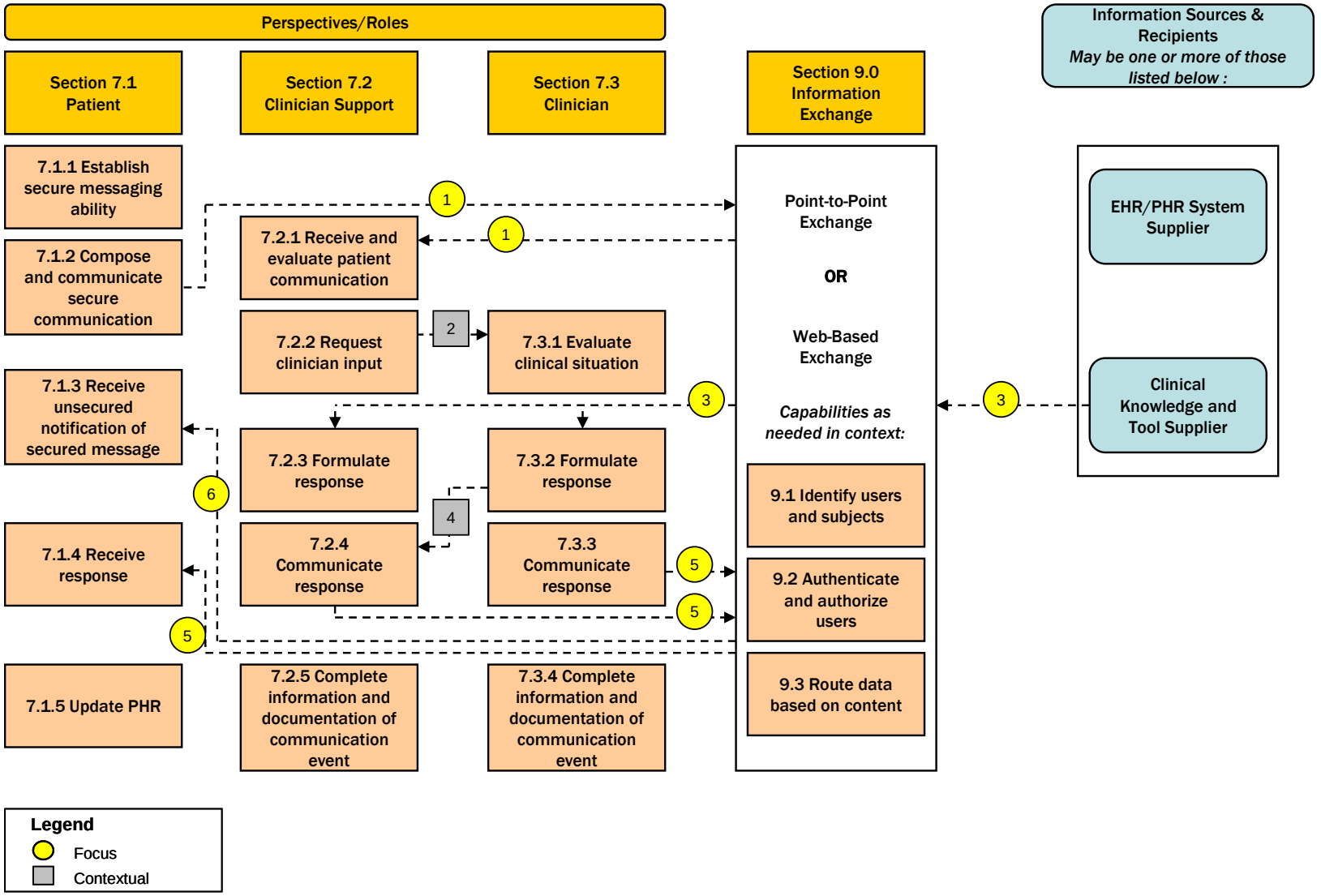
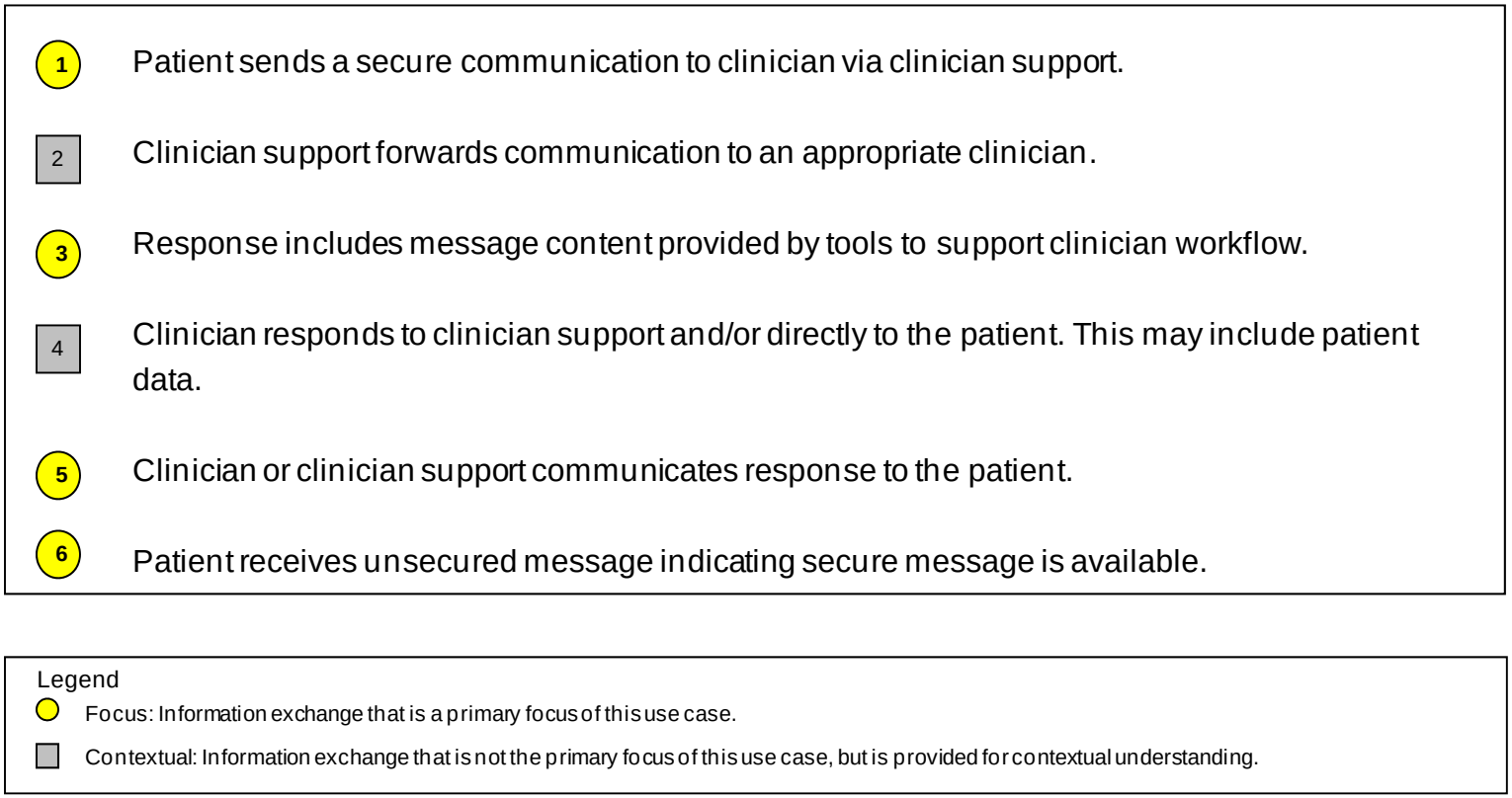


**Figure 7-2. Patient-Initiated Communication Scenario Flows**



## Figure 7-3. Patient-Initiated Communication, Patient Perspective

| Code | Description | Comments |
|---|---|---|
| **7.1.1** | **Event:** Establish secure messaging ability | |
| **7.1.1.1** | **Action:** Establish required authorization and authentication. | To use secure messaging capabilities, patients need to be authenticated. This is sometimes done by having a face-to-face meeting in which a patient presents proof of identity. A part of the process is also to verify that a patient is authorized to use this capability and has signed necessary documents (e.g., waivers and terms and conditions for use). These processes may be established as a part of an existing relationship between the patient, the clinician, and a secure messaging tool supplier.<br><br>Similarly, there is an expectation that all users of secure messaging, including clinicians and clinician support staff, will be appropriately authorized and authenticated. |
| **7.1.1.2** | **Action:** Establish user identification code, password, and other security measures to enable access to secure messaging. | After authentication and authorization, a user identification code (user id) and password are established for a patient that will enable use of this capability. Other security measures may also be imposed that a patient will need to satisfy. |
| **7.1.1.3** | **Action:** Conduct training and other remaining set-up as needed. | Users may also require some training on the use of these secure messaging tools. These tools can include tools built around an EHR, PHR, patient portal, or other communication tools. There may also be additional set-up tasks required to establish the secure messaging capability. |
| **7.1.2** | **Event:** Compose and communicate secure communication | **Figure 7-1, Flow 1** |

| Code | Description | Comments |
|---|---|---|
| **7.1.2.1** | **Action:** Compose message using tools established to support secure communication. | Patients use the secure messaging tool to compose a communication to one or more clinicians. This will typically include logging into the secure messaging tool using the user id, password, and other security measures previously established.<br><br>Secure messages can be structured messages, unstructured messages, or a mixed format. Structured content may benefit patients and clinicians by providing guidance that will make for complete, efficient, easily understood communications. On the other hand, a structure may inhibit patients from being able to “tell their own story” in terms that are more familiar and conversational which may allow for more patient-provided information.<br><br>Communications may also include additional materials as appropriate (attachments, links to internet sites, etc.). |
| **7.1.2.2** | **Action:** Send secure communication. | Once composed, a secure message can be sent to a clinician, and this corresponds to Figure 7-1, Flow 1. In some implementations, communications sent to a specific clinician may, in fact, be received by clinician support staff (or a message "triage" group) who supports a clinician by reviewing the communication to ascertain whether it can be satisfied by someone other than a clinician (such as an administrative request) or needs to be directed to the intended clinician.<br><br>Communication tools may also include some message tracking capabilities (e.g., Read Receipt, Guaranteed Delivery) to give patients additional ability to see who has read the communication and what action has taken place with respect to it. |
| **7.1.3** | **Event:** Receive unsecured notification of secure message | **Figure 7-1, Flow 6** |

| Code | Description | Comments |
|---|---|---|
| **7.1.3.1** | **Action:** Receive unsecured notification of secure message. | Once a clinician has responded to a patient communication, the clinician's response is made available through the same secure messaging tool. Since patients may not regularly log in to their secure messaging tool, an unsecured email message may be sent to the patient (on an unsecured channel designated by the patient) indicating that a secure message is waiting to be read. This corresponds to Figure 7-1, Flow 6.<br><br>This unsecured message does not include any sensitive patient data. It also does not include a link to the secure messaging tool due to potential security risks (e.g., "phishing"). |
| **7.1.4** | **Event:** Receive response | **Figure 7-1, Flow 5** |
| **7.1.4.1** | **Action:** Receive secured message from clinician. | A patient logs in to the secure messaging tool using the appropriate user id and password. The patient reads the secure message. This corresponds to Figure 7-1, Flow 5.<br><br>The clinician's message may include a text, related materials, and links to additional information. Structured messaging may also help patients understand clinician responses by organizing the clinician's content into broad categories of information such as problems reported, possible explanations, recommendations, where to look for additional information, etc. |
| **7.1.5** | **Event:** Update PHR | |

| Code | Description | Comments |
|---|---|---|
| **7.1.5.1** | **Action:** Update PHR or other patient tool with results of communication and response. | After reading a clinician's response to a secure message, the patient may update existing personal health records, noting the details of the interaction. Structured messages and messaging tools may support this type of patient activity. The patient may also take other clinical actions as appropriate based on the communication.<br><br>Secure messaging tools typically include the ability for the system to automatically track communications sent and received, providing an audit trail of communications and the ability to revisit past communications as necessary. |

## Figure 7-4. Patient-Initiated Communication, Clinician Support Perspective

| Code | Description | Comments |
|---|---|---|
| **7.2.1** | **Event:** Receive and evaluate patient communication | **Figure 7-1, Flow 1** |
| **7.2.1.1** | **Action:** Receive patient communication. | A secure communication from a patient is received by clinician support staff, and this corresponds to Figure 7-1, Flow 1.<br><br>Secure messaging tools may also include the ability for the tool to automatically link the patient communication with the appropriate electronic medical records to assist in efficient communication workflow and processing. |
| **7.2.1.2** | **Action:** Evaluate patient communication. | Clinician support makes an initial assessment of the patient communication to separate communications that require clinical action from those that can be addressed through other support (e.g., administrative support).<br><br>As above, structured messaging tools may support workflow for these messages. |
| **7.2.2** | **Event:** Request clinician input | **Figure 7-1, Flow 2** |
| **7.2.2.1** | **Action:** Confirm receipt and evaluation of patient communication. | A message receipt confirmation may be automatic by the secure messaging tool. This is intended to alert the patient that the communication has been received and read.<br><br>If the communication can be processed with minimal clinician input such as those that are primarily administrative in nature, a planned response may be developed by clinician support and discussed with the clinician. |
| **7.2.2.2** | **Action:** Forward patient communication to clinician(s). | If further clinician input is required, the original patient communication may be forwarded by clinician support to a clinician, potentially with a preliminary assessment. This corresponds to Figure 7-1, Flow 2. |

| Code | Description | Comments |
|---|---|---|
| **7.2.3** | **Event:** Formulate response | **Figure 7-1, Flow 3** |
| **7.2.3.1** | **Action:** Determine appropriate clinical response. | A response to the communication may be developed by clinician support. This response may or may not include input from clinicians depending on the patient communication and its evaluation. A phone discussion between clinician support and the patient may also be included within this action to determine the most appropriate response. |
| **7.2.3.2** | **Action:** Compose communication response. | Once the most appropriate action is determined, the communication response is created. Message content support tools may further aid in workflow by providing practice-specific or clinician-specific "pre-packaged" content and this corresponds to Figure 7-1, Flow 3.<br><br>The communication response may also include additional materials as appropriate (e.g., attachments, educational materials, links to internet sites). |
| **7.2.4** | **Event:** Communicate response | **Figure 7-1, Flow 4 and Flow 5** |
| **7.2.4.1** | **Action:** Transmit communication response. | Once the communication response is composed by clinician support, it is sent through the secure messaging tool. This corresponds to Figure 7-1, Flow 4 and Flow 5.<br><br>This transmission action can also automatically trigger an unsecured message to the patient, providing notification that a secured message is available. |
| **7.2.5** | **Event:** Complete information and documentation of communication event | |

| Code | Description | Comments |
|---|---|---|
| **7.2.5.1** | **Action:** Complete medical information related to this communication exchange. | Communications sent by and to the patient may require an update to the patient's medical records. In some cases, selected insertion of the patient communication content may be possible. These tools may also support an automatic linkage between messages and the patient's medical record.<br><br>Secure messaging tools provide automatic logging of communications sent and received for audit logs and subsequent review. |
| **7.2.5.2** | **Action:** Complete documentation of communication. | There may be additional actions required to complete this communication event. Automated tools may assist and promote clinician workflow to minimize this work. |

## Figure 7-5. Patient-Initiated Communication, Clinician Perspective

| Code | Description | Comments |
|---|---|---|
| **7.3.1** | **Event:** Evaluate clinical situation | **Figure 7-1, Flow 2** |
| **7.3.1.1** | **Action:** Evaluate patient communication and clinical situation. | The secure message is received by the clinician through an initial notification that an incoming message exists and then the actual message can be read and processed. This corresponds to Figure 7-1, Flow 2.<br><br>Secure messaging tools may also include the ability to automatically link the patient communication with the appropriate electronic medical records to assist in efficient processing.<br><br>Once the message is read by a clinician, an initial evaluation of the patient's clinical situation is made. The patient's medical record and other resources may be considered. |
| **7.3.2** | **Event:** Formulate Response | **Figure 7-1, Flow 3 and Flow 4** |

| Code | Description | Comments |
|---|---|---|
| **7.3.2.1** | **Action:** Determine appropriate clinical response. | A response to the communication may be developed by the clinician or by the clinician support team based on input from the clinician. This corresponds to Figure 7-1, Flow 3 and Flow 4. Additional information from the patient may be gathered to determine the most appropriate response. |
| **7.3.2.2** | **Action:** Compose communication response. | Once the most appropriate action is determined, the communication response is created. Structured messaging tools may assist in formulating the response. In addition, message content support tools may further aid in workflow by providing practice-specific or clinician-specific "pre-packaged" content. If clinicians or their support teams frequently send certain types of communications, these content tools can improve workflow.<br><br>The communication response may also include additional materials as appropriate (e.g., attachments, educational materials, links to internet sites). Attachments should not require any specialized tools for patients to open them, but only technologies that are readily available in home and other non-clinical environments. |
| **7.3.3** | **Event:** Communicate response | **Figure 7-1, Flow 5** |
| **7.3.3.1** | **Action:** Transmit communication response. | Once the communication response is composed by the clinician, it is sent through the same communication tool. This corresponds to Figure 7-1, Flow 5.<br><br>This transmission action can also automatically trigger an unsecured email message to the patient, providing notification that a secured message is available. |
| **7.3.4** | **Event:** Complete information and documentation of communication event | |

| Code | Description | Comments |
|---|---|---|
| **7.3.4.1** | **Action:** Complete medical information related to this communication exchange. | Communications sent by and to the patient may require updating the patient's medical records. In some cases, selected insertion of the patient communication content may be possible. These tools may also support an automatic linkage between messages and the patient's medical record.<br><br>Secure messaging tools provide automatic logging of communications sent and received for audit logs and subsequent review. |
| **7.3.4.2** | **Action:** Complete documentation of communication. | There may be other systems and processes that require completion related to this communication. Automated tools may assist and promote clinician workflow to minimize this work. |

# 8.0 Scenario 2: Clinician-Initiated Communication

**Figure 8-1. Clinician-Initiated Communication**

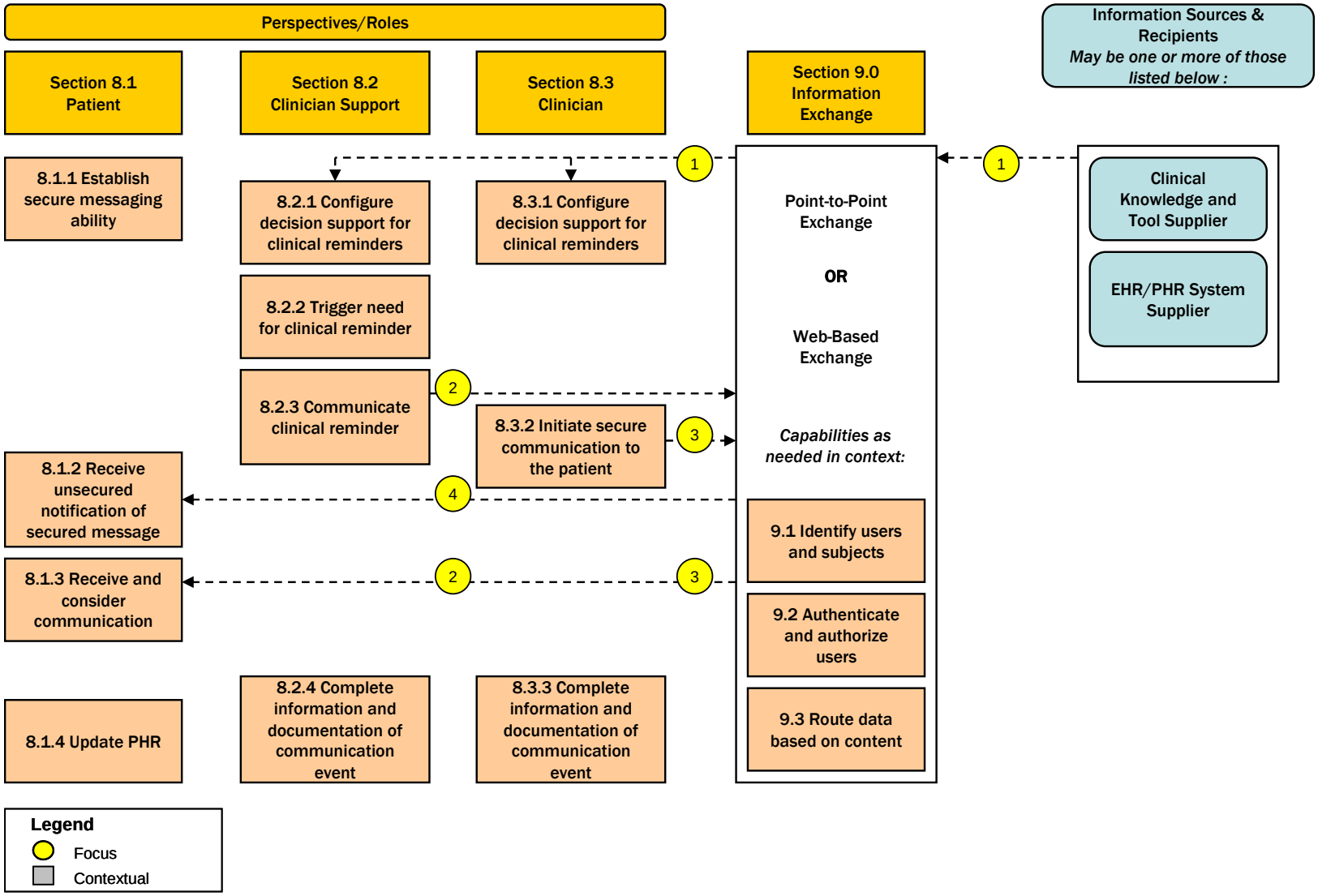
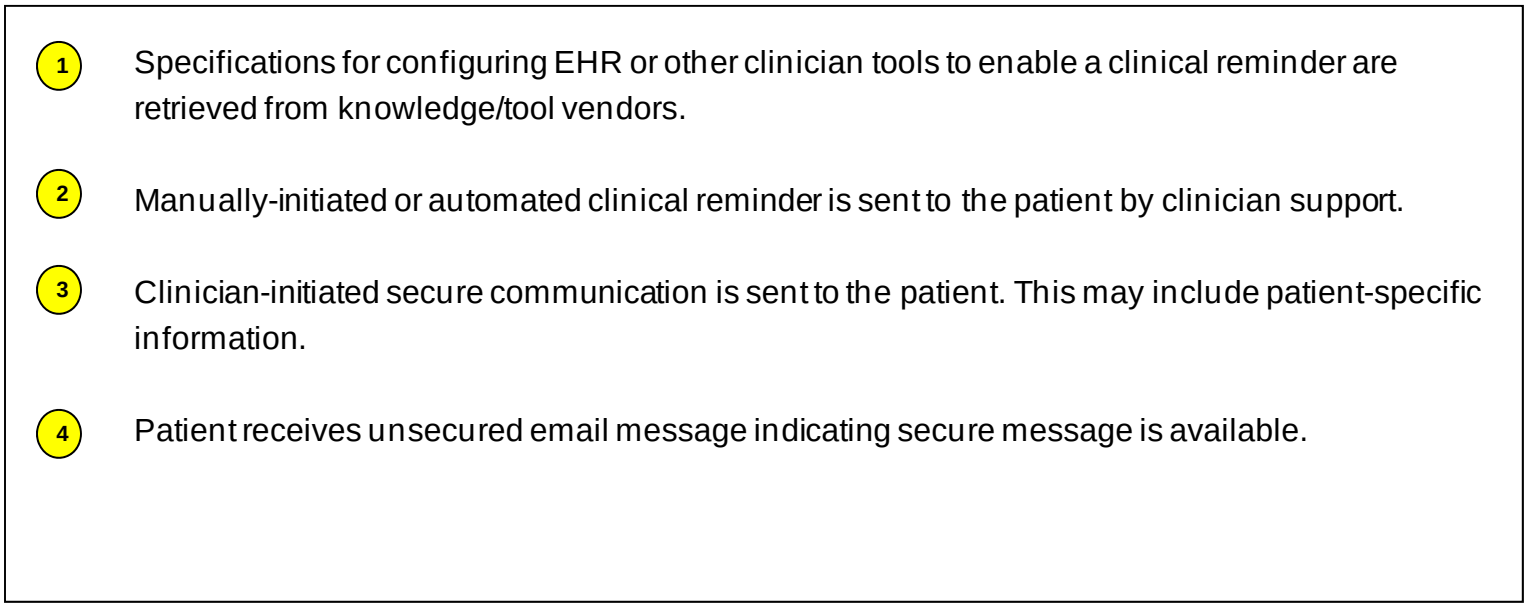


**Figure 8-2. Clinician-Initiated Communication Scenario Flows**



## Figure 8-3. Clinician-Initiated Communication, Patient Perspective

| Code | Description | Comments |
|---|---|---|
| **8.1.1** | **Event:** Establish secure messaging ability | |
| **8.1.1.1** | **Action:** Establish required authorization and authentication. | To use secure messaging capabilities, patients need to be authenticated. This is sometimes done by having a face-to-face meeting in which a patient presents proof of identity.<br><br>A part of the process is also to verify that a patient is authorized to use this capability and has signed necessary documents (e.g., waivers and terms and conditions for use).<br><br>Similarly, there is an expectation that all users of secure messaging, including clinicians and clinician support staff, will be appropriately authorized and authenticated. |
| **8.1.1.2** | **Action:** Establish user identification code, password, and other security measures to enable access to secure messaging. | After authentication and authorization, a user identification code (user id) and password are established for a patient that will enable use of this capability in the future. Other security measures may also be imposed that a patient will need to satisfy. |
| **8.1.1.3** | **Action:** Conduct training and other remaining set-up as needed. | Users may also require some training on the use of these secure messaging tools. These tools can include access through EHR, PHR, patient portal, or other communication tools. This training may include instructions on how to gain additional support in the future including the use of a help desk. There may also be additional set-up tasks required to establish the secure messaging capability. |
| **8.1.2** | **Event:** Receive unsecured notification of secured message | **Figure 8-1, Flow 4** |

| Code | Description | Comments |
|---|---|---|
| **8.1.2.1** | **Action:** Receive unsecured notification of secure message. | When a clinician sends a secure message communication, it is made available through the patient's secure messaging tool. Since a patient may not regularly log in to this tool, frequently an unsecured email message is sent to the patient (on an unsecured channel designated by the patient) indicating that a secure message is waiting to be read. This corresponds to Figure 8-1, Flow 4.<br><br>This unsecured email message does not include any sensitive patient data. It also does not include a link to the secure messaging tool due to potential security risks (e.g., "phishing"). |
| **8.1.3** | **Event:** Receive and consider communication | **Figure 8-1, Flow 2 and Flow 3** |
| **8.1.3.1** | **Action:** Receive secured message from clinician. | The patient logs in to the secure messaging tool using the appropriate user id and password and reads the secure message. This corresponds to Figure 8-1, Flow 2 and Flow 3.<br><br>The clinician's message may include text, related materials and attachments, and links to additional information. Structured content may also help patients understand clinician responses. |
| **8.1.3.2** | **Action:** Consider communication. | The patient considers the content of the clinician message and takes appropriate actions. This may include creating a patient-initiated secure message for the clinician. For example, if this clinician message is a reminder for a preventive health activity, the patient may initiate the process for making an appointment to complete that activity. |
| **8.1.4** | **Event:** Update PHR | |

| Code | Description | Comments |
|---|---|---|
| **8.1.4.1** | **Action:** Update PHR or other patient tool with results of communication and response. | After reading a clinician's secure message, the patient may update existing personal health records, noting the details of the interaction. Structured messages and messaging tools may support this type of patient activity.<br><br>Secure messaging tools typically include the ability for the system to automatically track communications sent and received, providing an audit trail of communications and the ability to revisit past communications as necessary. |

## Figure 8-4. Clinician-Initiated Communication, Clinician Support Perspective

| Code | Description | Comments |
|---|---|---|
| **8.2.1** | **Event:** Configure decision support for clinical reminders | **Figure 8-1, Flow 1** |
| **8.2.1.1** | **Action:** Receive decision support information on clinical reminders. | Vendors and other sources may provide reference information to clinicians and their organization to support clinical reminders. This corresponds to Figure 8-1, Flow 1. |
| **8.2.1.2** | **Action:** Incorporate decision support for clinical reminders. | The EHR could use this clinical reminder information to implement a reminder capability for an organization based on support and guidance from clinicians and a clinician support team. Clinicians and the clinician support team incorporate this information into the EHR to support the clinical reminder capability. |
| **8.2.2** | **Event:** Trigger need for clinical reminder | |
| **8.2.2.1** | **Action:** Activate a clinical reminder message based on patient data. | After installation and depending on an organization's preference, EHRs may trigger clinical reminder messages based on patient data. This can be implemented to occur with or without clinician intervention.<br><br>The need for a clinical reminder could be based on patient age, demographic data, clinical condition, or other information contained in a patient record. In some cases, the trigger for this reminder may be automatically transmitted by the EHR to assist in clinician workflow and promote patient health.<br><br>This functionality could also trigger reminders to a group of patients (e.g., seasonal flu shot reminder). |
| **8.2.3** | **Event:** Communicate clinical reminder | **Figure 8-1, Flow 2** |

| Code | Description | Comments |
|---|---|---|
| **8.2.3.1** | **Action:** Compose a clinical reminder. | A clinical reminder could be automatically created based on a patient data trigger or may be created by a clinician or clinician support.<br><br>The reminder could include several types of content including patient specific data, pre-packaged content, and additional content specific to this reminder. The reminders could include additional materials as appropriate (e.g., educational materials, links to internet sites).<br><br>It may be beneficial to allow clinicians and clinician support staff to indicate a need for a future follow-up to verify patient activities, such as whether a clinical reminder was read or another specific action, such as scheduling an appointment, was taken. This capability is also supportive of clinician workflow and patient health.<br><br>These reminders could be created once and sent to more than one recipient. For a given patient, this could include other members of a patient support team (e.g., family member, care coordinator). Messages could also be sent to multiple patients as long as the privacy of each patient was protected. |
| **8.2.3.2** | **Action:** Transmit communication response. | Once the communication response is composed, it may be sent through the secure messaging tool. This corresponds to Figure 8-1, Flow 2.<br><br>This transmission action can also automatically trigger an unsecured message to the patient, providing notification that a secured message is available. |
| **8.2.4** | **Event:** Complete information and documentation of communication event | |

| Code | Description | Comments |
|---|---|---|
| **8.2.4.1** | **Action:** Complete medical information related to this communication exchange. | Communications sent by and to the patient may require updating the patient's medical records. In some cases, selected insertion of the patient communication content may be possible. These tools may also automatically attach all communications to and from the patient to the patient's medical record.<br><br>Secure messaging tools could provide automatic logging of communications sent and received for audit logs and subsequent review. |
| **8.2.4.2** | **Action:** Complete documentation of communication. | There may be other systems and processes that require completion related to this communication. Automated tools may assist and promote clinician workflow to minimize this work. |

**Figure 8-5. Clinician-Initiated Communication, Clinician Perspective**

| Code | Description | Comments |
|---|---|---|
| **8.3.1** | **Event:** Configure decision support for clinical reminders | **Figure 8-1, Flow 1** |
| **8.3.1.1** | **Action:** Receive decision support information on clinical reminders. | Vendors and other sources may provide reference information to clinicians and their organization to support clinical reminders. This corresponds to Figure 8-1, Flow 1. |
| **8.3.1.2** | **Action:** Implement decision support for clinical reminders. | The EHR could use this clinical reminder information to implement a reminder capability for an organization based on support and guidance from clinicians and a clinician support team. Clinicians and the clinician support team incorporate this information into the EHR to support the clinical reminder capability. |
| **8.3.2** | **Event:** Initiate secure communication to the patient | **Figure 8-1, Flow 3** |

| Code | Description | Comments |
|---|---|---|
| **8.3.2.1** | **Action:** Compose a secure communication. | Clinicians use the secure messaging tool to compose a communication to one or more patients. This will typically include logging into the secure messaging tool using the user id, password, and other security measures previously established.<br><br>Communications may also include additional materials as appropriate (e.g., attachments, links to internet sites). |
| **8.3.2.2** | **Action:** Transmit a secure communication. | Once composed, a secure message can be sent to one or more patients. This corresponds to Figure 8-1, Flow 3.<br><br>Communication tools may also include some message tracking facilities (e.g., Read Receipt, Guaranteed Delivery) to give clinicians the additional ability to see who has read the communication. |
| **8.3.3** | **Event:** Complete information and documentation of communication event | |
| **8.3.3.1** | **Action:** Complete medical information related to this communication exchange. | Secure messaging tools could provide automatic logging of communications sent and received for audit logs and subsequent review.<br><br>Communications sent by and to the patient may require updating the patient's specific medical records. These tools may also automatically attach all communications to and from the patient to the patient's medical record. |
| **8.3.3.2** | **Action:** Complete documentation of communication. | There may be other systems and processes that require completion related to this communication. Automated tools may assist and promote clinician workflow to minimize this work. |

# 9.0 Information Exchange

This section highlights selected information exchange capabilities which enable the scenarios described in this use case. These functional capabilities may be provided fully or partially by secure messaging tools as well as information exchange capabilities provided by a variety of organizations including free-standing or geographic health information exchanges (e.g., Regional Health Information Organizations), integrated care delivery networks, provider organizations, health record banks, public health networks, specialty networks, and others supporting these capabilities.

**Figure 9-1. Patient-Provider Secure Messaging Information Exchange Capabilities**

| Code | Capability | Comments |
|---|---|---|
| **9.1** | Identify users and subjects | Capability to identify a person without repudiation. For example, a secure message sent by the clinician to the consumer is matched to the appropriate individual by the secure messaging tool or other information exchange capability. |
| **9.2** | Authenticate and authorize users | Capability to confirm the identity of an individual requesting access to a system either through authentication or via attestation of third party authentication. For example, if a patient uses a portal-based secure messaging tool, the processes of identity proofing and authentication would likely be managed directly by the administrative functions of the portal. If an information exchange capability is used to access secure messaging services, it may be possible that the patient authenticates to a different system (e.g., their personally controlled health record) which then communicates with the secure messaging service, and attests to the authentication of the user. |
| **9.3** | Route data based on content | Capability to securely deliver data to the intended recipient, confirm delivery and receipt, including the ability to route data based on message content if required. For example, routing may be involved in delivering a notification advising the patient that there is a secure message from the clinician available for review. |

While not described in this section, other capabilities that support information exchange include: data integrity and non-repudiation checking; subject and user identity arbitration with like identities during information exchanges; access logging and error handling for data access and exchange; consumer review of disclosure and access logs; and routing consumer requests to correct data.

**Point-to-Point Exchange:** Point-to-point exchange includes direct interactions between two systems which do not involve intermediary information exchange functions to route and deliver the data. For the purposes of this use case, the two points could be located in different messaging applications accessed by a patient or a clinician. Similarly, the patient and clinician could be supported by two different access points within a single application or architecture (e.g., a patient portal supporting messaging by the patient and an EHR supporting messaging by a clinician within a single closed integrated care delivery network).

**Web-Based Exchange:** An exchange of information supported by the Internet or World Wide Web. For the purposes of this use case, secure messaging capabilities for patients and providers may be supported by separate distinct applications that rely on the Internet to transmit secure messages.

# 10.0 Dataset Considerations

In discussing secure messaging, the related topics of message content, message processing, and "structured messaging" may be worth noting. While secure messages are a valuable capability for enhancing the patient – provider relationship, message content can vary greatly and can be highly, or minimally, structured. This section discusses some of these considerations regarding message content and degrees of structuring.

Messages can include structured and unstructured content, or a combination of the two. Certain content such as adult patient age might be more amenable to being limited by a structure that would restrict input to an integer number of years. Other content (e.g., patient's chief complaint) might be better served through unstructured free text. Likewise, structuring methods (e.g., the use of drop-down boxes or other familiar web-based presentation techniques) may be relevant for this discussion. This use case does not attempt to prescribe the use of structured or unstructured content for any particular type of message transaction.

This section describes message content for sample message types or transactions that could be included as secure messages. In addition, this list attempts to define which transactions might be amenable to more or less structure as currently understood. Each of these communications would include certain structured elements such as patient identifying information, provider identifying information, date and time of message, message priority, and message subject. These broad message descriptor data (e.g., message "metadata") are separate from the additional message content described below. Finally, a group of industry subject matter experts may be convened to analyze these issues and questions further. This group may conduct this type of analysis and report on their conclusions.

Potential information needs relevant for this use case are discussed below.

**Patient Inquiries/Questions**

General medical question – These communications are perhaps the least amenable to structure since, by definition, the range of questions that could be communicated is completely unknown. Free text is probably most appropriate in this situation though it may still be useful to include categories of information that might be relevant for any and all questions.

New medical issue – A patient may want to report on, or ask about, a new medical problem. A particular set of data such as symptoms or possibly relevant problem background may be useful to help with initial clinical consideration. These data may be similar to what might be asked during a patient interview during a face-to-face visit or what clinician support staff might ask during a telephone advice line

conversation. Clearly, some free text as a part of this communication may be appropriate.

Question about medical tests/procedures – Patients who receive medical test results or are considering future treatments or procedures may have specific questions or comments about them. Some of this information could be requested and conveyed within the context of patient educational information, and a structure that reflects the range of tests, procedures, and/or treatments may be most appropriate. A free text "additional comments" option may be appropriate at the end of the communication.

**Patient-Provided Data**

Existing medical issue – Similar to above, patients may have information to report about a known condition for which there are new data. As an example, this type of transaction may be related to remote monitoring of a chronic condition. As above, some level of structure may assist in this communication and in fact may be more relevant given it is a known condition. Some free text may be appropriate for this type of transaction.

Pre-visit data capture and communication – One possible use of secure messaging is for the capture of information from the patient as a head-start for obtaining the information normally gathered during the initial patient interview. As such, there is a significant set of data that could be gathered, according to a specific structure. Items such as personal medical history, family medical history, allergies, current medications, and other topics could be candidates for this structuring. Free text may be appropriate within some of these areas. General free text outside of this structure may not be appropriate or useful.

**Patient Service Request**

Referral request – Patient requests for referrals for additional services may be an area in which a highly structured interaction with a clinician might be appropriate. Free text may add limited value to this interaction.

Prescription renewal request – A patient request to have a prescription renewed, perhaps when the number of prescribed refills has been exhausted, is a common need that could be satisfied by a highly structured communication. Specific data needs for this communication might include prescription number, prescription date, number of refills ordered and filled, pharmacy identifying information, and other data. In addition, the Centers for Medicare & Medicaid Services (CMS) ePrescribing initiative would have a bearing on the appropriate data for consideration within this transaction. Free text may have limited value to this interaction.

### Clinician-Initiated Communications

Post-visit summary – Another use for secure messaging is that of a provider-initiated communication that summarizes a recent face-to-face visit. As a part of patient visits, many providers are now including physical documents that accompany the patient at the end of a visit. These materials could also be included within a secure message. Sample data types could include patient measurements, diagnoses, treatments, prescribed medications (with explanation of rationale for prescription, side-effects, etc.), home care instructions, and other patient education materials. Free text may also be appropriate.

Clinical reminders – Providers, or their surrogates, may initiate messages for patients that remind patients of a possible need for a regular appointment or a wellness activity. Cancer screenings, annual checkups, and other reminders may best serve the needs of patients and providers, and be accomplished through the use of highly structured secure messages. Free text would probably not be utilized as many of these messages may be automatically generated by an EHR.

New data relevant for patient(s) – Providers, or their surrogates, may initiate messages for patients and their surrogates to make them aware of new information which may be related to new research, new drugs, or new treatments.

In addition to the information needs listed above, several categories of information needs exist that are currently considered out of scope for this use case. They are discussed below.

### Out of Scope for this Use Case

Appointment request – Patient requests for appointments are a popular use for secure messages but are outside the scope of this use case which is focused on clinical messaging rather than administrative needs. Similarly, messages confirming appointments, appointment reminders, and appointment change and cancellation messages would be appropriate when these transactions are addressed.

Billing questions – Communication that relate to billing questions are possible but are also outside the scope of this use case. The focus is on clinical communications rather than financially-related communications.

Patient profile updates – Secure communications could also address patient needs to update data on their demographics, however these communications are outside the scope of this use case.

Other administrative questions – Secure communications that address other administrative questions are also out of the scope of this use case.

# Appendix A: Glossary

These items are included to clarify the intent of this use case. They should not be interpreted as approved terms or definitions but considered as contextual descriptions. There are parallel activities underway to develop specific terminology based on consensus throughout the industry.

**AHIC:** American Health Information Community; a federal advisory body chartered in 2005, serving to make recommendations to the Secretary of the U.S. Department of Health and Human Services regarding the development and adoption of health information technology.

**CCHIT:** The Certification Commission for Healthcare Information Technology; a recognized certification body for electronic health records (EHR) and their networks, as well as an independent, voluntary, private-sector initiative. CCHIT's mission is to accelerate the adoption of health information technology by creating an efficient, credible, and sustainable certification program.

**Clinical Knowledge and Tool Suppliers:** Organizations that provide knowledge and tools to aid in the understanding and treatment of health and disease conditions. These tools may include knowledge regarding items such as clinical reminders, decision support, expertise, and research findings. The tools encompass a wide range of capabilities that may be useful and available to patients, consumers, clinicians, and other health professionals. These tools can also support secure messaging, educational materials, and messaging content. These suppliers may include developers, providers, resellers, operators, and others who may provide these or similar capabilities.

**Clinical Support Staff:** Individuals who support the workflow of clinicians. For this use case, this may be by receiving and evaluating communications from consumers or patients, and then engaging the appropriate clinician in the response to the patient.

**Clinicians:** Healthcare providers with patient care responsibilities, including physicians, advanced practice nurses, physician assistants, nurses, psychologists, pharmacists, and other licensed and credentialed personnel involved in treating patients.

**CMS:** Centers for Medicare & Medicaid Services; a federal agency within the Department of Health and Human Services that administers Medicare, Medicaid, and the State Children's Health Insurance Program.

**Consumers:** Members of the public that include patients as well as caregivers, patient advocates, surrogates, family members, and other parties who may be acting for, or in support of, a patient receiving or potentially receiving healthcare services.

**Department of Health and Human Services (HHS):** The United States federal agency responsible for protecting the health of the nation and providing essential human services with the assistance of its operating divisions that include: Administration for Children and Families (ACF), Administration on Aging (AOA), Agency for Healthcare Research and Quality (AHRQ), Agency for Toxic Substances and Disease Registry (ATSDR), Centers for Disease Control and Prevention (CDC), Centers for Medicare & Medicaid Services (CMS), Food and Drug Administration (FDA), Health Resources and Services Administration (HRSA), Indian Health Services (IHS), National Institutes of Health (NIH), Program Support Center (PSC), and Substance Abuse and Mental Health Services Administration (SAMHSA).

**Electronic Health Record (EHR):** An electronic, cumulative record of information on an individual across more than one healthcare setting that is collected, managed, and consulted by professionals involved in the individual's health and care. This EHR description encompasses similar information maintained on patients within a single care setting (a.k.a., Electronic Medical Record (EMR)).

**Electronic Health Record (EHR) / Personal Health Record (PHR) System Suppliers:** Organizations which provide specific EHR and PHR solutions to clinicians and patients such as software applications and software services. These suppliers may include developers, providers, resellers, operators, and others who may provide these or similar capabilities.

**FDA:** Food and Drug Administration; a federal agency within the Department of Health and Human Services responsible for the safety regulation of foods, dietary supplements, vaccines, drugs, medical devices, veterinary products, biological medical products, blood products, and cosmetics.

**Health Information Exchange (HIE):** The electronic movement of health-related data and information among organizations according to specific standards, protocols, and other agreed criteria. These functional capabilities may be provided fully or partially by a variety of organizations including free-standing or geographic health information exchanges (e.g., Regional Health Information Organizations (RHIOs)), integrated care delivery networks, provider organizations, health record banks, public health networks, specialty networks, and others supporting these capabilities. This term may also be used to describe the specific organizations that provide these capabilities such as RHIOs and Health Information Exchange Organizations.

**Healthcare Entities:** Organizations that are engaged in or support the delivery of healthcare. These organizations could include hospitals, ambulatory clinics, long-term care facilities, community-based healthcare organizations, employers/occupational health, school health, dental clinics, psychology clinics, care delivery organizations, pharmacies, home health agencies, hospice care providers, and other healthcare facilities.

**Healthcare Payors:** Insurers, including health plans, self-insured employer plans, and third party administrators, providing healthcare benefits to enrolled members and reimbursing provider organizations.

**HITSP:** The American National Standards Institute (ANSI) Healthcare Information Technology Standards Panel; a body created in 2005 in an effort to promote interoperability and harmonization of healthcare information technology through standards that would serve as a cooperative partnership between the public and private sectors.

**ONC:** Office of the National Coordinator for Health Information Technology; serves as the Secretary's principal advisor on the development, application, and use of health information technology in an effort to improve the quality, safety, and efficiency of the nation's health through the development of an interoperable harmonized health information infrastructure.

**Patients:** Members of the public who receive healthcare services.

**Personal Health Record (PHR):** An electronic, cumulative record of health-related information on an individual, drawn from multiple sources, that is created, collected, and managed by the individual or an agent acting for the individual. The content of and rights of access to the PHR are controlled by the individual or agent. The PHR is also known as the electronic Personal Health Record (ePHR).

**Point-to-Point Exchange:** Point-to-point exchange includes direct interactions between two systems which do not involve intermediary information exchange functions to route and deliver the data. For the purposes of this use case, the two points could be located in different messaging applications accessed by a patient or a provider. Similarly, the patient and provider could be supported by two different access points within a single application or architecture (e.g., a patient portal supporting messaging by the patient and an EHR supporting messaging by a clinician within a single closed integrated care delivery network).

**Web-Based Exchange:** An exchange of information supported by the Internet or World Wide Web. For the purpose of this use case, secure messaging capabilities for patients and providers may be supported by separate distinct applications that rely on the Internet to transmit secure messages.