Secure, Obligated and Coordinated Collaboration in Health Care for the Patient-Centered Medical Home

Solomon Berhe, MS[1], Steve Demurjian, PhD[1], Rishi Saripalle, MS[1], Thomas Agresta, MD[2], Jing Liu, BSE[1], Antonio Cusano, BSE[1], Andal Fequiere, BSE[1], Jim Gedarovich ,BSE[1]

[1]Department of Computer Science & Engineering, University of Connecticut, Storrs, CT;
[2]Department of Family Medicine, University of Connecticut Health Center, Farmington, CT

Abstract

In the patient-centered medical home, PCMH, patient care is overseen by a primary care physician leading a team of health care providers, who collaborate to optimize treatment. To facilitate interactions in PCMH, secure collaboration will be needed to: control access to information; dictate who can do what when; and promote sharing and concurrent access. This contrasts approaches such as the National Institute of Standard and Technology (NIST) role-based access control (RBAC), where the emphasis is on controlling access and separating responsibilities. This paper investigates secure collaboration within an application such as PCMH, through: a futuristic scenario for patient care; proposed collaboration extensions to the NIST RBAC standard with a fine-grained obligated mechanism and workflow; and a prototype of PCMH via the Google Wave real-time collaboration platform.

1 Introduction

Over the next decade there will likely be a shift in the management of care for patients with chronic conditions towards the patient-centered medical home (PCMH) collaborating with an Accountable Care Organization (ACO), to facilitate care coordination within a multidisciplinary team headed by a primary care physician (PCP) [1,2,5,7]. One objective is to improve the coordination of care amongst providers which needs timely information sharing. This is often a barrier, resulting in preventable deaths and adverse outcomes from medical errors and drug interactions [10,11]. One potential solution is a *virtual chart (VC)* [13] that aggregates patient data from multiple sources via Health Information Exchange (Fig. 1).

In order to improve the quality of care, workflow based solutions have been proposed and implemented [18], but face numerous issues. First, most medical workflow solutions focus on patient needs, medical data, or scheduled tasks [12]. These approaches might be ideal for specialized coordination and data sharing within a practice or a hospital; but workflow solutions for the PCMH and ACO must integrate patient flow, tasks flow, teams, and inter-institutional flow, to facilitate/enforce collaboration. Second, workflows are often designed where collaboration is on a voluntary basis [9], with providers interacting ad-hoc by phone and other means; an *obligation mechanism* [4, 15] is needed for timely participation to insure collaborating providers "sign-off". Third, the participation in such workflows must be simple and in different formats (e.g., PC, Smartphone, PDA, etc.). If institutions need to install software, servers, hire administrative staff, etc., then the desire to use such a system may be limited. While not the subject of this paper, the need to provide integrated and easy-to-use repositories of patient data, in a form most suitable to each provider, will be vital for acceptance and wide-scale usage [6]. Fourth, such complicated and integrated solutions bring new security challenges. If medical data is shared in such a highly collaborative setting, privacy and security concerns must be addressed at multiple levels.

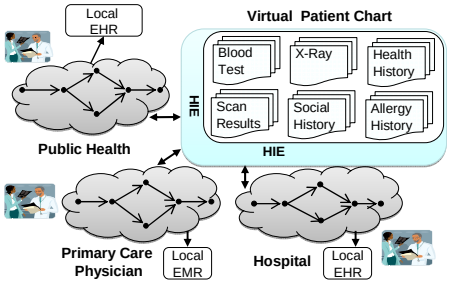


Figure 1. Collaboration in a PCMH.

This paper explores secure collaboration for a PCMH and ACO, requiring the coordination of providers, constrained by how and when they interact. Section 2 presents a futuristic health care scenario. Section 3 reviews our proposed extensions to the NIST RBAC standard, expanding our work [4] on collaboration with an obligation mechanism and workflow. Section 4 presents a prototype using Google Wave to demonstrate the collaboration and coordination within PCMH, which also illustrates our security extensions from Section 3. Section 5 offers concluding remarks.

2 Health Care Scenario

In this section, we present a futuristic scenario that illustrates episodes of collaborative/coordinated care. The year is 2020 and Mr. Smith is a 58 year old patient with diabetes and a history of smoking who presents to the ER with new onset severe shortness of breath, wheezing and fever after returning from a business trip to Asia. On exam, the patient has some findings consistent with pneumonia, congestive heart failure and emphysema; the ER physician orders an EKG, X-ray and lab studies which show an elevated white blood count, a pulmonary infiltrate with evidence of heart failure, and a rapid irregular heart rate. The patient quickly deteriorates and has significant hypoxia. The ER nurse asks the patient to authorize a request for current health records, authenticated with a password and biometric data. Systems are accessed to generate a virtual chart (Fig. 1) which displays all appropriate data along with patient alerts, e.g., patient wishes to be temporarily placed on a ventilator if needed, has a penicillin allergy and an enzyme deficiency that affects metabolism of certain drugs.

The ER physician gets alerted by the CDC to the fact that an emerging infectious disease is suspected from where the patient had traveled and appropriate precautions for staff are initiated. The Primary Care physician (PCP) is notified of the admission via a direct connection to the EMR and a secure message to her cell phone/PDA, providing access to test results and the ER Physician from the out of state conference she is attending. A cardiologist is consulted collaboratively by the PCP and ER physician and participates in a real-time review of the EKG and appropriate lab studies to determine that use of a new medication for atrial fibrillation and heart failure is not indicated given the patients' risk from the enzyme deficiency. He is started on the specific antibiotic recommended by the CDC. The treatment team collaborates amongst themselves synchronously and asynchronously during his hospital stay viewing the same health data from their own perspectives. This coordination results in more timely and effective care allowing the patient to return to home a few days later.

The PCP, hospitalist physician and visiting nurse communicate directly with each other through a collaboration portal for discharge planning. They agree that the patient would benefit from a nurse coming to his home twice per week which is instantaneously arranged, the insurance company, and the nursing agency, triggered by the hospitalist generating a discharge summary and follow-up requests. This is sent to the patient's PCP, the Nursing agency (updating their respective EMR's),and to the patients PHR.

The patient monitors his vital signs daily, and adjusts medications based on these to prevent a recurrence of the heart failure. He records these into his PHR, which automatically flags his PCP if he falls outside specified parameters. The PCMH team reviews his course since discharge, current medications and symptoms, and maps out a treatment/monitoring plan. The scenario demonstrates a need for: team-based, time-constrained, and location-independent collaboration; real-time communication; secure/shared access to a virtual chart; and patient data/medical request and flow.

3 Extensions to NIST RBAC

The NIST reference model [16], in the top half of Fig. 2, provides: $RBAC_0$ to link the concepts of roles and permissions (permission assignment) and users and roles (user assignment); $RBAC_1$ for role hierarchies where privileges are available to other roles via inheritance; and, $RBAC_2$ which adds separation of duty (SOD) through mutual exclusive (ME) roles and permissions [14]. SOD and ME prevent access; this contrasts with the needs of the PCMH, where we want to define who can/must collaborate with whom at what times and under what constraints to share information and coordinate actions. Our prior work extended NIST RBAC with Collaboration on Duty (COD) [4]. This section reviews this effort and further extensions for an obligation mechanism and workflow, focusing on relevant concepts, rather than a formal model.

The underlying core of the extensions to NIST RBAC involves the definition of a collaboration, its steps, and its workflow, constrained under certain conditions. In Fig. 3, a collaboration team (T) based on the Section 2 scenario, represents interacting users each with a specific role participating in actions against a set of objects in a workflow. The *collaboration workflow* is a sequence of linked *collaboration steps (cs)*. The example in Fig. 3 goes through steps cs1 to cs5: Triage (assess patient), Test (order tests), Review EKG, Read X-Ray, and Discuss Results. A subset of users, roles, authorizations, objects, and permissions are:

- **Users = {ERPhysician1, ERNurse1, EKGTech1, XRayTech1, Cardiologist1, Cardiologist2, PCP1, etc.}**
- **Roles = {Physician, Nurse, EKGTech, XRayTech, Radiologist, Cardiologist, Patient, PCP, etc.}**
- **User Authorizations = {(ERPhysician1, Physician), (ERNurse1, Nurse), (XRayTech1, XRayTech), (Radiologist2, Radiologist), (PCP1, PCP), etc.}**
- **Objects = {o** $_{J.Smith}^{VC}$ **, o** $_{J.Smith}^{X-Ray}$ **, o** $_{J.Smith}^{EKG}$ **, "J. Smith", etc.}**
- **Medical Actions = {read, write, done, request, upload, etc.}**
- **Patient Actions = {toXRayRoom, toEKGRoom, intake, discharge, etc.}**

- **Permissions = {P_0 = (intake, "J. Smith"), P_1 = (request, $o^{VC}_{J.Smith}$), P_2 = (request, $o^{X-Ray}_{J.Smith}$), P_3 = (request, $o^{EKG}_{J.Smith}$), P_4 = (toXRayRoom, "J. Smith"), P_5 = (toEKGRoom,"J. Smith"), P_6 = (done, null), P_7 = (upload, $o^{X-Ray}_{J.Smith}$), P_8 = (upload, $o^{EKG}_{J.Smith}$), P_9 = (read, $o^{EKG}_{J.Smith}$), P_{10} = (read, $o^{X-Ray}_{J.Smith}$), P_{11} = (discharge, "J. Smith"), etc.}**

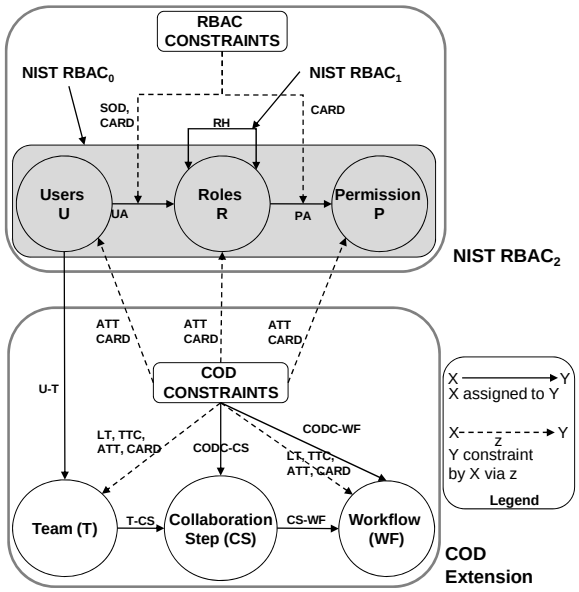


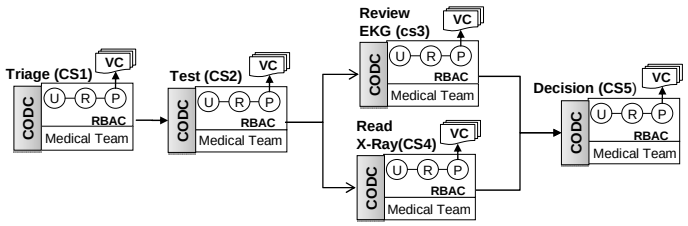
Figure 2: NIST RBAC (top) with Extensions (bottom).

The next extension is *collaboration on duty constraints (CODC)*, in the bottom half of Fig. 2, that dictate the conditions under which a collaboration or step occurs, e.g., the actions of the users with their allowed permissions (by role) constrained by time (when can the collaboration occur) and participation (who can or must collaborate). There are four different CODCs: *lifetime (LT)* for when the collaboration is active; *time-to-complete (TTC)* for the maximum duration of the collaboration; c*ardinality (CARD)*, a range (min, max) of roles (users) who must participate and permissions that must be activated in the collaboration; and, *attendance (ATT)* for the required participation of users in the collaboration. Constraints defined at the collaboration step restrict the team in the particular step, while at the workflow level restrict all teams.

The final issue is to determine when a collaboration step is activated and completed depending on both the actions that are performed against objects and permissions and the particular user or role that initiates the action. These actions represent an *obligation of participation*, e.g., in Fig. 3 at least one cardiologist must participate in CS5. For a workflow to be activated at least one of its collaboration steps must be activated which requires its team to be activated. This is accomplished by the team members who participate by activating their permissions (medical action, patient action) through their role. The completion of a collaboration step depends upon the CODCs defined, also dictating the obligation to participate. A user's duty is completed when all of the required permissions are activated by the user through its role. A role's duty is completed when all its required permissions are activated. A permission is completed when all required permissions are activated. A team is completed when all required permissions are completed. Lastly, a workflow is completed when all paths from source to sink are completed and all constraints are met (Fig. 3).

4 Prototype Efforts in Google Wave

To support enforcement of collaborative security, we are experimenting with Google Wave [8], which provides a rich set of primitives for real-time collaboration (data and communication) for a set of individuals operating as a team, supporting both location and platform independence. Waves allow for the sharing of information (all kinds and types) with real-time interactions (video, audio, and chat). A *wave* provides a context for the collaboration, with the ability to playback earlier portions of the collaboration; for a PCMH, a provider could reply the actions in an earlier decision. While Google Wave provides the communication infrastructure, it offers no specific security solutions to support RBAC or our extensions for collaboration, obligation, and workflow. Security policies in Google Wave are coarse grained, i.e., a participant either can see the complete content or none. There is no concept of workflow where waves can be considered as nodes in a directed graph towards a common goal, as given in Fig. 3. Moreover, participation of providers is on a voluntary basis. From a privacy perspective the main limitation of a wave is that shared medical data would permanently reside in the wave, accessible to all (unless controlled by application code), which is not a suitable solution in applications such as PCMH.



	Medical Teams	Required Users and Roles	Required Permissions
CS1	T1 = {ERPhysician1, ERNurse1, ERNurse2}	Physician Nurse	P_0; P_1; P_3; P_4; P_5; P_6
CS2	T2 = {EKGTech1, XRayTech1}	EKGTech, XRayTech	P_6; P_7; P_8
CS3	T3 = {Radiologist1, Radiologist2}	Radiologist	P_6; P_{10}
CS4	T4 = {Cardiologist1, Cardiologist2}	Cardiologist	P_6; P_9
CS5	T5 = T1 U T3 U T4 U {PCP1}	Physician; Cardiologist Radiologist; PCP1	P_1; P_9; P_{10}; P_6; P_{11}

Figure 3: Collaboration Scenario.

However, the Google Wave API allows the integration of Wave *gadgets* as a means to embed non-trusted code that customizes the Wave look and feel. Gadgets would be useful in a medical application to allow patient data to be organized and structured for presentation to providers (or to embed virtualized GUIs from EMRs). For our purposes, we are using Google Wave gadgets to support the various actions in Fig. 3, to: create separate collaboration steps; to represent the workflow between steps; to enforce RBAC, COD constraints, and obligations; to oversee the collaboration team; and, to assure that no medical data resides in the wave permanently.

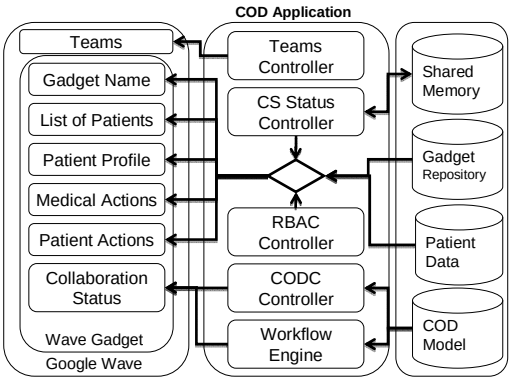


Figure 4: COD Prototype Architecture.

Fig. 4 presents the detailed COD prototype software architecture, which brings together the concepts as discussed in the earlier sections of the paper. The workflow engine in Fig. 4 is in charge of activating and deactivating collaboration steps based on whether the collaboration constraints are met (Section 3 and Fig. 3). A deactivated gadget screen displays no data and prohibits any medical or patient actions (the collaboration step is not enabled). An activated screen displays shared data: a patient drop-down list from which one patient is selected; the patient's profile, medical history, notes; further medical data that needs to be requested (X-Ray, EKG); and, the next step of how to proceed with the patient (Fig 5C). Each screen contains a list of completed/awaiting actions (Fig 5D).

Since waves and gadgets cannot communicate with one another directly, the mechanism that enforces the activation/deactivation of screens is implemented using shared memory (Fig. 4) to track completed and uncompleted collaboration steps. This requires the client gadgets to use a pull approach and actively listen to the shared memory to activate/deactivate its screen. For flexible workflows and to simplify administration, the Publisher-Subscriber paradigm is used. Collaboration steps to be activated after a particular step is completed (publish) listen for completion (subscribe). If a step's flag turns to "completed", the COD application switches all subscribers' status to "activate" and enforces it by loading the list of patients into the GUI. To illustrate this and other capabilities, we present in Fig. 5 Google Wave screens that implement the collaboration as discussed in Section 2 and shown in Fig. 3 which is communicated through an intermediate COD application (Fig. 4).

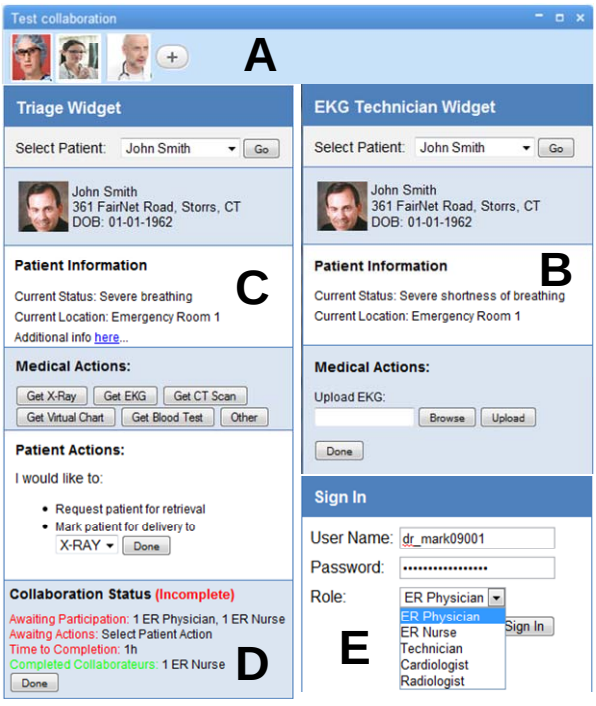


Figure 5: Screenshots of Prototype.

From an enforcement perspective, we have prototyped three mechanisms for controlling RBAC, workflows, and obligations via gadgets. Gadgets are publically

available, therefore the first mechanism insures that only authorized personal can access the gadget repository. The RBAC policies assign each role a set of gadgets; upon logon, a user must provide the correct credentials as illustrated in Fig. 5E. The second mechanism focuses on RBAC policies. Once the correct gadget is loaded, each team member (Fig. 5A) has limited privileges in terms of viewing the medical data and authorized actions, e.g., in Fig. 3, the ER physician can order an EKG or X-Ray while the ER nurse can only view Mr. Smith's medical history, alerts and reminders. The third mechanism is for obligation constraint checking, and activation and deactivation of collaboration steps (Fig. 5D), which are achieved through gadgets and the shared memory (Fig. 4). In the example, each collaboration step is limited through time and coordination constraints (Fig. 4 – CODC Controller, WF Engine, Shared Memory and CS Status Controller). After the EKG and XRay tests (CS2) are completed, the technician's gadget (Fig. 5C) removes Mr. Smith and the Cardiologist (CS3) and Radiologist (CS4) gadgets become active with Mr. Smith populated in the patient list (not shown). Overall, these three mechanisms facilitate protection of medical data/actions based on user credentials, user role and (active/inactive) collaboration step.

5 Conclusion

In this paper, we have presented secure, obligated and coordinated collaboration issues for PCMH and ACO, which require solutions that transcend tradition models and: emphasize collaboration, constrain access, promote obligated participation, and enforce workflow (see Section 3). We detailed our ongoing prototyping effort that leverages a real-time collaboration toolkit, Google Wave, which has been customized via application specific data/software to represent the PCMH/ACO and scenario (Section 2 and Fig. 3). We believe the work presented herein is a critical first step to understand secure collaboration for healthcare in a PCMH/ACO setting. Our ongoing research involves: formalizing all collaboration extensions given in Section 3; designing administrative security analyses for individual collaborations and their interaction (e.g., users who participate in many different collaborations); and exploring the usage of the Unified Modeling Language (UML) and our prior work on access control extensions to UML [17].

References

[1] AAFP, [Online], 2010 [cited 2010 March 12]. Available from: URL: www.aafp.org/

[2] AAP, [Online], 2010 [cited 2010 March 12]. Available from: URL: www.medicalhomeinfo.org/

[3] ACP, [Online], 2010 [cited 2010 March 12]. Available from: URL: http://www.acponline.org/advocacy/where_we_stand/medical_home/

[4] Berhe S, Demurjian S, Agresta T. Emerging Trends in Health Care Delivery: Towards Collaborative Security for NIST RBAC, Proc. of the 23rd Conf. on Data and Appl. Sec., 2009, 283- 290.

[5] Clancy C, Anderson C, White P. Investing in health information infrastructure: can it help to achieve health reform? Health Affairs, 28(2), 2009, 478-482.

[6] Demurjian S, Saripelle R, Berhe S. An Integrated Ontology Framework for Health Information Exchange. Proc. of the 21st Intl. Conf. on SE & Knowledge Engineering, 2009, 575-580.

[7] Gold M, [Online] [cited 2010 March] Accountable care organizations: will they deliver? Available from: URL: www.mathematica-mpr.com/publications/pdfs/health/account_care_orgs_brief.pdf

[8] Google, [Online] 2010 [cited 2010 March 12]. Available from: URL:code.google.com/apis/wave/

[9] Hoshi K, Waterworth J. Effective Collaboration for Healthcare by Bridging the Reality Gap across Media-Physical Spaces, Proc. of Conf. on Pervasive Technologies Related to Assistive Environments, 2008.

[10] Institute of Medicine, To err is human: building a safer health system, National Academy Press, 2000.

[11] Institute of Medicine, Crossing the quality chasm: a new health system for the 21st century, National Academy Press, 2001.

[12] Institute of Medicine, The future of drug safety: promoting and protecting the health of the public, National Academy Press, 2006.

[13] Kenny P, Parsons T, Gratch J, Rizzo A. Virtual Humans for Assisted Health Care, Proc. of 1st Intl. Conf. on Pervasive Technologies Related to Assistive Environments, 2008.

[14] Li N, Tripunitara MV, Bizri Z. On mutually exclusive roles and separation-of-duty, ACM Trans Inf Syst Security, 2007; 10(2), 42-51.

[15] Ni Q, Bertino E, Lobo J. An obligation model bridging access control policies and privacy policies, Proc. of the 13th ACM Symp. on Access Control Models and Technologies, 2008, 133-142.

[16] NIST RBAC, [Online] 2010 [cited 2010 March] Available from: URL:csrc.nist.gov/groups/SNS/rbac

[17] Pavlich-Mariscal J, Demurjian S, Michel L. A Framework for Component-Based Enforcement for Access Control, Proc. of 27th Intl. Conf. of Chilean Computer Science Society, 2008, 13-22.

[18] Song X, Hwong B, Matos G, Rudorfer, et al. Understanding requirements for computer-aided healthcare workflows: experiences and challenges. In Proc. of the 28th Intl. Conf. on SE, 2006, 930 – 934.