Event-Based Data Dissemination Control in Healthcare

Jatinder Singh and Jean Bacon

Computing Laboratory
University of Cambridge
firstname.lastname@cl.cam.ac.uk

Abstract. There is a movement in healthcare towards preventative care. This shift involves using technology to assist in care provision outside traditional care institutions - for instance, in a patient's home. To support such an environment, care providers require notification of incidents as they occur. However, health information is sensitive, thus the circumstances for disclosure must be controlled.

This paper provides an overview of our work on event-based data dissemination control in healthcare. We describe the nature of data-driven healthcare, and how care providers meet their data management responsibilities through fine-grained, context-aware policy rules that control the information they release.

1 Introduction

Current healthcare is organised around *acute* (reactive) care, catering for the urgent requirements of patients [1]. However, *chronic* conditions, requiring management over a period of time, consume a large proportion of healthcare resources [2]. With the ageing population, there is a global push to better manage such conditions. The way forward is through innovation, improving the use of information and focusing on preventative care [3].

Care services are becoming increasingly pervasive, where monitoring technologies are fast becoming integral to the care process. Sensors measure physiological state, allowing care outside of traditional care institutions (i.e. at the patient's home rather than in hospital). Such technologies assist in the early identification of health issues, and provide alerts in situations requiring response (e.g. emergencies). This brings benefits to patients, through improved care and quality of life, while reducing the burden on health services.

Healthcare is highly collaborative, where health providers require information in order to deliver care services. The environment is data-driven, in the sense that care providers require notification when particular incidents occur. However, health information is sensitive, and remains so over time. Thus, it must be protected. To balance these concerns, it is necessary to consider the context in which information is shared. That is, what information is appropriate to be shared in the particular circumstances.

D. Weerasinghe (Ed.): eHealth 2008, LNICST 1, pp. 167–174, 2009.

This paper presents an overview of how an event-based (publish/subscribe) middleware can be extended for use in a health environment. We begin by detailing event-driven healthcare, focusing particularly on homecare environments. We then discuss the sensitivity of health data, followed by a description of how context-aware policy rules can be built into the infrastructure to control the circumstances for information disclosure. We conclude by describing how to effect communication across administrative boundaries, in line with the general NHS goals of local control, flexibility and responsibility for care providers.

2 Event-Driven Healthcare

Healthcare is a highly collaborative environment, where information sharing is crucial to the provision of care. It is common that a GP refers a patient to a specialist, or to a hospital; that prescriptions are sent to a pharmacy clearing service (EPS); that certain information flows to accountants for the purposes of billing. These interactions occur across administrative domains, where each may provide a different service as part of the care process.

Homecare[1] involves providing care services for patients outside of traditional care institutions (e.g. a hospital). Sensor technologies provide detailed representations of patient state: alerting of particular incidents (i.e. emergencies) [4] and reducing the need for human intervention. Detailed physiological information assists in the early detection of issues, which may improve treatment, reducing the need for institutional care services [3]. Preventative care improves resource allocation, reducing the burden on health services [5]. The patient enjoys greater independence, requiring less institutional time (e.g. hospitals, surgeries for 'checkups') [5], while receiving more information to assist in self-care (patient empowerment) - a goal of the NHS [3].

2.1 Incidents in Homecare

Homecare environments are small and dynamic, created on demand to cater for specific aspects of a patient's well-being [6]. As such, each homecare instance is customised to the particular situation, in terms of management policy and the service providers (entities) involved. Homecare is highly data-driven: *entities* deliver services as part of the care process, requiring notification of *incidents* as they occur. Incidents include actions performed, such as a nurse administering a treatment or a patient taking a drug; observations, such as sensor monitoring reports; and state changes, such as the detection of an emergency situation.

Existing outside of traditional institutions (e.g. a hospital), homecare domains are particularly amenable to utilising care services from multiple providers. Entities require access to *relevant* information to perform their duties; depending on factors such as their role in the care process, credentials, managing organisation, in addition to patient particulars (conditions, demographics) and the current environmental state (e.g. well-being). That is, the information required by an entity to provide a service is dependent upon circumstance.

[1] The term *homecare* is used as it is expected that the home will be the primary environment for patient management. However, care might encompass mobile technologies that monitor or provide feedback while the patient is outside their home.

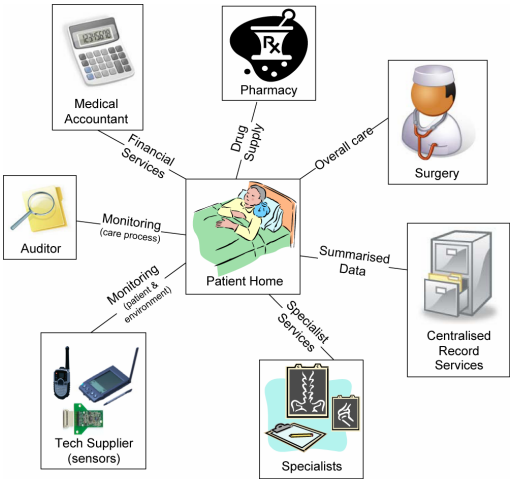

Fig. 1. Home healthcare involves interactions between entities, managed in different administrative domains, each delivering specific services as part of the care process

Infrastructure must support the active dissemination of information (incidents) while providing the means to control information disclosure, in an environment of federated administrative policy.

3 Healthcare Information Protection

Healthcare information, somewhat paradoxically, must be shared, yet protected. Notions of patient confidentiality underpin the carer-patient relationship, an ideal imposed by law [7]. Consent is the basis for sharing information, which may be implied (usually when directly concerning treatment) [8]. Carers are responsible for upholding the confidentiality of information obtained as part of the care process, and will be held accountable if information is mismanaged.

Medical professionals take this responsibility seriously. Many have expressed concerns over the risk posed to patient confidentiality by centralised record systems [9]. A goal of the NHS is to give local providers a greater degree of freedom to manage their services [10]. Local providers want control over the information they manage, as reflected in a recent BMA survey where 81% of respondents were against storing their local surgery data in centralised databases [11].

Care providers must share information to afford proper care. However, providers are responsible for protecting personal medical information. To balance these concerns, information must be shared as *appropriate* to the situation, taking into account: consent, the service the entity provides and their relation to the patient, the expected information requirements (level of detail) and the current environmental state (e.g. emergency). The mechanisms outlined here allow notions of local control to extend to information sharing, by providing the means for policy to define the circumstances in which information is communicated.

4 Event-Based Middleware

Event-based architectures suit data-driven scenarios, e.g. homecare, where principals require notification of the incidents (events) which occur within a system.

4.1 Middleware

Middleware provides a level of indirection between applications and a network infrastructure, through which all communication must pass. An *event* is a data-rich encapsulation of an incident that represents a particular semantic. Event-based middleware notifies those interested in receiving particular information as the event occurs within the system. Middleware is an appropriate point to enforce data control policy as it ensures automatic compliance by applications.

4.2 Publish/Subscribe

Publish/subscribe [12] is an asynchronous messaging paradigm suited to event-driven environments. A principal takes the role of a publisher and/or a subscriber. Subscribers register their interest in receiving particular information through a subscription. Publishers produce events (information) independent of subscribers. Principals communicate through event brokers, which route events from publishers to subscribers. Through a process called notification, events are delivered to subscribers with matching subscriptions. Essentially, a subscriber requests particular information, which is delivered by the middleware upon the publication of an event matching that request.

A key feature of the paradigm is that information producers and consumers are decoupled. This saves burdening producers with the addressing specifics of every information sink. Instead, consumers declare their interest in receiving particular information, leaving the middleware to deliver relevant publications.

We have coupled a publish/subscribe middleware into a database management system, to allow a database to act as a messaging broker [13]. This allows a broker to produce and consume events, facilitates data replication through a common type interface and allows rich representations of state (e.g. through stored data and functions). This database-broker integration provides an appropriate point for enforcing data management polices.

4.3 Interaction Control

Interaction control refers to the customisation of data to circumstance [14]. It involves loading policy rules into a broker to define the situations for data release. Three types of policy rules function to control data[2]:

Subscription authorisation. These define the circumstances in which a user may subscribe (request) particular information for delivery as it occurs. An example rule might allow a Doctor to subscribe to Treatment events, but only for patients that he treats.

[2] A detailed description is provided in [15]. See Section 6 for examples.

Event restriction. These rules define the conditions in which certain events are restricted (not delivered) for an active subscription. For example, a rule might prevent a particular doctor from receiving events concerning a patient's HIV treatment. Restrictions are imposed silently, to not reveal to the subscriber any sensitive information encoded in the restriction itself. Restriction differs from subscription authorisation, in that it stops propagation of particular information, even if the subscription channel (general request) is authorised and established.

Event transformation. Transformations involve altering an event instance, changing attributes, values or the event type to better satisfy the information requirements of the subscriber, current context, etc. That is, the content of the information can be customised to suit the particular circumstances.

Policy rules are enforced in a broker to bring about information control. Rules are context-aware, referencing various aspects of state, including 1) messaging substrate information (principals connected, event content), 2) user credentials (e.g. roles held) and/or 3) environmental state (referencing local data or external services). It is these context-sensitive policy rules that allow fine-grained control over information dissemination, allowing policy to account for both general cases and exceptions (such as emergency overrides).

As the environment is event-driven, events themselves serve to alter environmental state. This means that the control mechanisms are responsive to changes in context. For example, if an event occurs meaning a doctor no longer has a relationship with a patient, then their subscription is deactivated (if appropriate).

Typical access control mechanisms are binary in nature: permit or deny. Transformation provides more, allowing aspects of an event to be changed; perturbing or enriching values or encapsulating a different semantic by converting an event into another type. This is a powerful mechanism that, in addition to allowing fine-grained control over information release, may also help with interoperability - mapping between the data models of applications and domains, and in providing summary data for surveys, such as epidemiological reports.

5 Cross-Domain Communication

Each administrative domain (e.g. doctors' surgery, specialist laboratory, hospital) maintains a broker[3] to serve as its point of communication. Entities producing information within a domain will publish events to their local broker. Events, subject to access policies, are delivered to the subscribers to this information, where a subscriber may be grounded in the local or an external domain.

Information flow is controlled through the definition of policy rules at its local broker, allowing each administrative domain fine-grained control over the circumstances for data release. This allows them to meet their responsibility for protecting patient information, sharing only in appropriate circumstances.

Entities seeking information receive it from the administrative domain responsible for that data. For example, a doctor seeking information on some test results will have their subscription satisfied by data from the relevant pathology domain. Both local

[3] Multiple brokers may facilitate communication; for simplicity we refer to one.

(domain-specific) and global (NHS-wide) services, such as the Electronic Staff Register, Legitimate Relationships and Patient Workgroups, can be used to identify information sources, in addition to providing information on which to base disclosure policies.

6 Health Scenarios

This section describes the application of our data control framework to two healthcare scenarios[4].

Drug auditing. This example, see Figure 2 A), shows how the Surgery domain controls the visibility of prescription information released to external parties. Homecare nurses may prescribe drugs, including controlled drugs (e.g. morphine) in certain circumstances [16]. Prescriptions must flow to the Electronic Prescription Service (EPS), without details of patient observations and the reason for the prescription (i.e. care record specifics). The supply of controlled drugs must be monitored by an auditor [17]. As the audit is prescriber focused, the auditor should not receive patient specifics unless the prescriber is under investigation[5].

Location privacy. Typical homecare scenarios use sensors to measure aspects of physiological state, transmitting this information to a remote store. Location sensors are common in such environments, and may detect the room of the house the patient

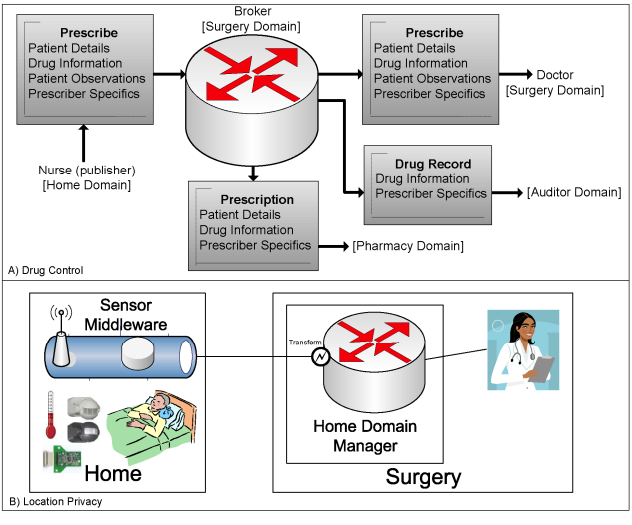

Fig. 2. A representation of the dataflows for the scenarios

[4] We model the Surgery as the information management domain, as it houses the doctor (case-manager) directly responsible for the care of the patient. In addition, it provides a more stable infrastructure than a home environment.

[5] To deal with this, the transformation rule creating the Drug_Record event is conditional on whether the prescriber is being investigated.

is in, or their GPS location. Precise location is important in emergencies, e.g. to inform A&E of where to dispatch the ambulance, and to help in the interpretation of sensor information (are they in bed? collapsed on the kitchen floor?). In the general case, a patient may prefer that their precise location is obscured. To interpret data, it may be sufficient to know whether the patient is in their familiar home environment, or elsewhere and thus subject to external stimuli. A single transformation rule can encapsulate these requirements, degrading the quality of location information except in emergency situations.

These examples highlight key features of the middleware. Firstly, that each domain manages its information: the Surgery domain meets its data handling responsibilities by only releasing that information required in the particular situation. It shows that one incident has relevance to many parties, where data visibility is managed within the infrastructure (cf. through applications). Further, we show how environmental state (context) can be used to alter the granularity of the information provided - as opposed to denying event transmission, hindering care, or transferring the complete event which raises privacy concerns.

7 Discussion and Conclusion

We have outlined a framework for controlling event-based information flow according to context. We feel that such an infrastructure provides a suitable base for managing information in data-driven healthcare environments.

Event-based paradigms, while effective for data dissemination, generally lack the rigorous access control mechanisms required by health infrastructure. By incorporating data control rules into the middleware layer, we force policy adherence. The integration of messaging and database systems allows for rich representations of context, while increasing performance by removing any communication overhead between the two substrates [13]. Further, health systems depend on theuse of database systems. By imposing a layer above technology commonplace, in NHS infrastructure, implementation and integration overheads are reduced.

Some recent debate concerns the use of centralised data stores. Our focus is on supporting the heterogeneous nature of the health service - where information flows across administrative domains. The NHS aims to give a greater degree of freedom and control to service providers. Our approach allows this notion to extend to the management of health information, giving those responsible for data fine-grained control over the circumstances for its release. Federated environments are scalable, and improve accountability by providing visibility of those responsible for information misuse or mismanagement (inadequate protection). The risks associated with centralised data stores are higher, as more users have the potential to access more information [18]. Care providers hold and require information relevant to their service, thus it is natural that they manage and are responsible for this information, respecting the privacy requests (consent) of their patients. Note that although this work is presented in the context of supporting environments of multiple, autonomous administrative domains, equally it can control data in more centralised architectures.

Future healthcare environments will be highly data-driven, involving interactions between patients, professionals, agents, sensors, etc. Infrastructure is required to allow

information to be shared, but also protected. We have presented methods to balance these concerns, by allowing information holders fine-grained control over the circumstances in which information is disclosed. This approach, built on common technology (database systems), supports the general NHS goal of local control and responsibility. Information protection is improved - responsibility means accountability. Federated data management not only mitigates against risks to confidentiality, but provides a realistic solution to managing the heterogeneous nature of the health service.

References

1. World Health Organisation: Innovative Care for Chronic Conditions (2002)
2. Department of Health (UK): Improving Chronic Disease Management (2004)
3. Department of Health (UK): Supporting People with Long Term Conditions. A NHS and Social Care Model to support local innovation and integration (2005)
4. Borriello, G., Stanford, V., Narayanaswami, C., Menning, W.: Pervasive computing in healthcare. IEEE Pervasive Computing 6(1), 17–19 (2007)
5. Department of Health (UK): Building Telecare in England (2005)
6. Singh, J., Bacon, J., Moody, K.: Dynamic trust domains for secure, private, technology-assisted living. In: ARES, pp. 27–34 (2007)
7. UK Crown: Data Protection Act (1998)
8. British Medical Association: Confidentiality and disclosure of information to PCTs in primary care settings (2007)
9. British Medical Association: Electronic health records will fail unless public and professional confidence is restored, says BMA (September 13 2007)
10. Darzi, L.: High quality care for all: NHS Next Stage Review (2008)
11. E-Health Insider: Medics sceptical about government data security (February 01, 2008)
12. Eugster, P., Felber, P., Guerraoui, R., Kermarrec, A.: The Many Faces of Publish/Subscribe. ACM Computing Surveys 35(2), 114–131 (2003)
13. Vargas, L., Bacon, J., Moody, K.: Event-Driven Database Information Sharing. In: British National Conference on Databases (BNCOD), pp. 113–125 (2008)
14. Bacon, J., Eyers, D.M., Singh, J., Pietzuch, P.R.: Access Control in Publish/Subscribe Systems. In: Distributed Event Based Systems, pp. 23–34 (2008)
15. Singh, J., Vargas, L., Bacon, J., Moody, K.: Policy-based information sharing in publish/subscribe middleware. POLICY, 137–144 (2008)
16. Department of Health (UK): Safer management of Controlled Drugs (2007)
17. UK Crown: The Controlled Drugs Regulations, UK (2006)
18. Anderson, R.J.: A security policy model for clinical information systems. In: IEEE Symposium on Security and Privacy, pp. 30–43 (1996)