Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

Note

Wireless Health and Care Security Requirements

Note no: DART/01/05

Authors: Ragni R. Arnesen, Jerker Danielsson, Jørn I. Vestgården and Jon Ølnes

Date: December 2004

Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

Norsk Regnesentral

Norsk Regnesentral (Norwegian Computing Center, NR) is a private, independent, non-profit foundation established in 1952. NR carries out contract research and development projects in the areas of information and communication technology and applied statistical modeling. The clients are a broad range of industrial, commercial and public service organizations in the national as well as the international market. Our scientific and technical capabilities are further developed in co-operation with The Research Council of Norway and key customers. The results of our projects may take the form of reports, software, prototypes, and short courses. A proof of the confidence and appreciation our clients have for us is given by the fact that most of our new contracts are signed with previous customers.

Norsk Regnesentral
Norwegian Computing Center
Postboks 114, Blindern
NO-0314 Oslo, Norway

Besøksadresse
Office address
Gaustadalléen 23
NO-0371 Oslo, Norway

Telefon · telephone
(+47) 22 85 25 00
Telefaks · telefax
(+47) 22 69 76 60

Internett · internet
www.nr.no
E-post · e-mail
nr@nr.no

Title	**WsHC Security Requirements**
Authors	**Ragni R. Arnesen, Jerker Danielsson, Jørn I. Vestgården and Jon Ølnes**
Date	December 2004
Year	2004
Publication number	DART/01/05

Abstract

This document lists the security threats that the general WsHC system model might be subjected to, and determines the security requirements of the WsHC system model.

Keywords	Wireless Health and Care, WsHC, Security Requirement, Security Threat
Target group	
Availability	Public
Project number	320302
Research field	Computer Security
Number of pages	13

Contents

1 Introduction

1.1 Document Content and Organisation

In the WsHC project several demonstrators are developed to show how technology can support different phases in a "wireless" health care scenario. Personally identifiable health information is by legislation classified as sensitive information, and must be protected with adequate security measures. The main goal of the security work package of WsHC is to develop a security architecture model that supports the needs of all the demonstrators.

This document contains security requirements, as well as functional requirements that have implications for the security architecture, of the demonstrators created in the project. The security requirements will serve as a basis for the design of a suitable security architecture. Note that safety requirements are not included in this document, except for some requirements related to integrity and availability of information.

1.2 About the Requirements

This document lists high-level main requirements, describes a general logical system model, and lists the requirements on this general model.

Requirements should be referred to like this: <number:> <actor(s):> <boldfaced tag>, e.g., "*Sec7: Patient data collector: Data integrity verification*."

1.3 Assumptions

Note the following assumptions:

- We assume the existence of a security policy that regulates access rights.
- We assume that there are mechanisms and interfaces for set-up and configuration, but have not set any requirements on these. This may be necessary to explore further.
- We assume the existence of systems for detecting failure of components and handle these, but do not set any requirements on failure modes.

2 System Properties and Requirements

2.1 Main Requirements

The main requirements are very high level and are shared between all demonstrators. Not all requirements are possible/desirable to solve through technological means. However, all the requirements are mandatory and should be satisfied by all demonstrators.

No.	*Requirement*
Main1	**Confidentiality.** Personally identifiable patient data shall not be disclosed to unauthorised actors

Main2	**Integrity**. Unauthorised actors shall not in any way be able to modify patient data or insert false data. (Note: Processed data should always be marked as such to distinguish it from original data.)
Main3	**Origin authentication**. It shall be possible to identify the origin of any action (create, write, read, delete) performed on patient data
Main4	**Availability**. Patient data within the system shall be available to authorised personnel at any time
Main5	**Patient identification.** The patient to whom the patient data pertains shall be identifiable
Main6	**Documentation.** Constraints (such as battery lifetime or geographic area) must be specified and delivery of patient data guaranteed within the constraints
Main7	**Patient notification.** A patient should be aware of what kind of data is collected from the patient, and for what purpose.

Note that patient data might be collected for statistical purposes, and in this case it is not necessary, and often not even legal, to identify the patient. Indeed, one might need additional measures to ensure the privacy of patients in such a setting. However, we do not consider this case here.

2.2 System Model

Figure shows a simple system model. All the demonstrators should fit into (parts of) this model. Note that the figure shows logical components; in an implementation their functionality can be distributed over several physical components, or several of them can be merged into the same physical component.

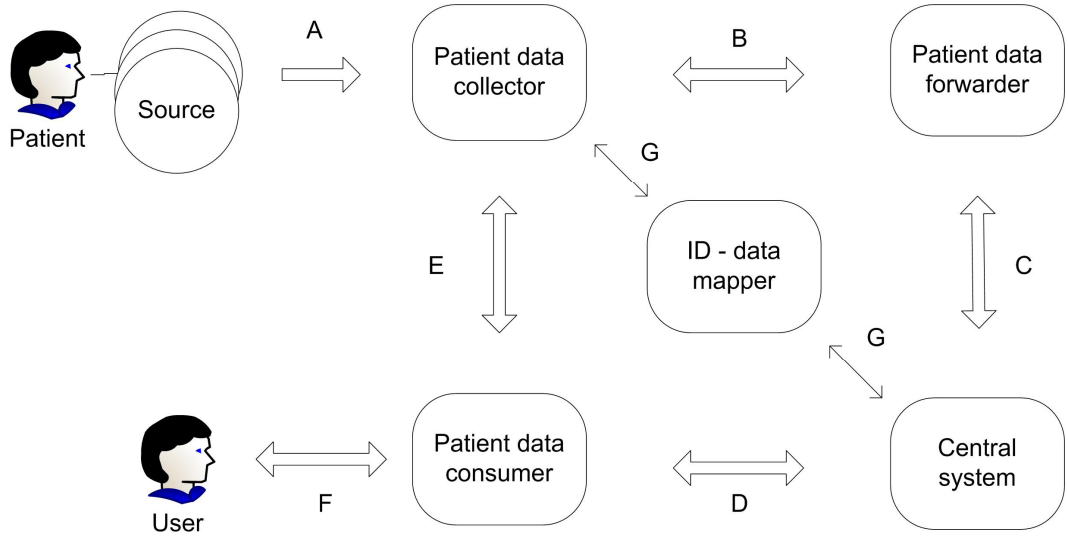

Figure1. Common System Model

Logical components and channels in the system model:

Source	Source of patient data, e.g. a sensor, storage unit, or user input through some interface. Patient data is sent to a Patient data collector (channel A). Simple data forwarders placed between the actual Source and the Patient data collector (such as the Sensor concentrator in the FieldCare demonstrator) are also treated as Sources in our model. Each Source is connected (physically or logically) to only one patient (at a time).
Patient data collector	Collects patient data from one or more Sources (channel A) and sends it to a Patient data forwarder (channel B) or directly to a Patient data consumer (channel E). The Patient data collector is a *trusted* entity that can handle unencrypted personally identifiable patient data (see requirement *Derived1: Patient data collector: Trusted entity*)
Patient data forwarder	Receives patient data (channel B) and forwards it to the Central system (channel C). The Patient data forwarder is *not* a trusted entity and should not handle unencrypted personally identifiable patient data (see requirement *Derived2: Patient data forwarder: Not trusted entity*)
Central system	Receives patient data (channel C) for processing or storage, and may send it to Patient data consumers (channel D).
Patient data consumer	Receives patient data (channel D or E) and displays it to users (channel F).
ID – data mapper	Determines the identity of the patient to whom patient data pertains and sends the identity to Patient data collector or Central system (channel G), depending on where it is implemented.

Assumptions:

- Channel A is a short-range wired/wireless communication link.
- Channel B may be an internal interface or a wired/wireless communication link.
- Channel C is a long-range wired/wireless communication link, possibly over a public network.
- Channel D may be any type of communication link, possibly over a public network.
- Channel E may be an internal interface or a wired/wireless short-range communication link. (Long-range communication between Patient data collector and Patient data consumer should be provided via the Central system.)
- Channel F is a visual display.
- Channel G is an internal interface in one of the components used to retrieve patient identity.

- Channels A through C transport patient data from Source to Central system. System management data may be sent in the same, and in the opposite, direction.
- Source has very limited capabilities of protecting the communication, e.g. no proper authentication of receiver.

2.3 Threats

No.	*Actor(s)*	*Threat*
Threat1	All components	Compromised or fake component (physical or logical attack)
Threat2	All components	Destroyed, lost, or stolen component
Threat3	All channels	Compromised or fake (components of) communication infrastructure (physical or logical attack)
Threat4	All channels	Unstable communication infrastructure (physical or logical attack, bad quality, accidents)
Threat5	All components	Software errors (failure in security mechanisms, routing, etc.)
Threat6	All components	Misuse of emergency access
Threat7	All channels	Eavesdropping of communication
Threat8	All components and channels	Denial of service attack (physical or logical attack, bad quality, accidents)

The threats may lead to the following unwanted consequences:

- Information unavailable
- Equipment unavailable (neither input nor output of data possible)
- Incorrect information (medical data, patient identity, sensor type, etc.)
- Sensitive information leaked

2.4 Functional Requirements

The following is a list of the functional requirements that have implications for the security architecture. There are thus many other functional requirements that are not included here. Note also that not all requirements are applicable to all demonstrators.

No.	*Actor(s)*	*Requirement*
Functional1	Source	**Replaceability**. It must be possible to replace a Source at any time

No.	*Actor(s)*	*Requirement*
Functional2	Patient data collector	**Replaceability**. It must be possible to replace a Patient data collector at any time
Functional3	Central system	**Transmit data.** Central system must be able to transmit stored data to remote terminals
Functional4	Source	**Patient mobility.** A Patient wearing Sources must be able to move freely around within a (preferably large) defined area without disruptions in the transmission of patient data
Functional5	Patient data collector	**Medical personnel mobility.** Medical personnel accessing data remotely must be able to move freely around within a (preferably large) defined area without disruptions in the transmission of patient data

2.5 Security Requirements

The following are security requirements on the logical system model. Note that not all requirements are applicable to all demonstrators.

No.	*Actor(s)*	*Requirement*
Sec1	Source	**Limited storage**. Source shall not store sent data longer than necessary (confidentiality)
Sec2	Channel A	**Short-range communication.** Source and Patient data collector shall only communicate with each other short range (confidentiality and integrity)
Sec3	Channel A	**Confidentiality protection.** Patient data should be protected from eavesdropping when transmitted to Patient data collector. (Note: communication is short range, which reduces the need for strong communication encryption)
Sec4	Channel A	**Integrity protection**. Patient data should be integrity protected when transmitted to Patient data collector. (Note: this includes protection from interference)
Sec5	Channel A	**No automatic roaming**. The connection between Source and Patient data collector shall be manually initiated, i.e. a human actor determines (at some point in time and through a defined procedure) which Sources and Patient data collectors that shall talk to each other (integrity)

No.	*Actor(s)*	*Requirement*
Sec6	Patient data collector	**Verify Source identity**. Patient data collector shall verify correct identity of the Source (integrity and accountability)
Sec7	Patient data collector	**Data integrity verification**. Patient data collector shall verify the integrity[1] of patient data (integrity)
Sec8	Patient data collector	**Data modification.** Patient data collector shall not modify patient data, except possibly for aggregation or other defined transformations (integrity)
Sec9	Patient data collector	**No unauthorised data access.** Patient data collector shall not give unauthorised actors access to patient data (confidentiality and integrity)
Sec10	Patient data collector	**Limited storage.** Patient data collector shall not store data longer than necessary to ensure successful transmission of patient data (confidentiality)
Sec11	Channels B, C, D and E	**Confidentiality protection.** Personally identifiable patient data shall be protected from eavesdropping when transmitted across open networks.
Sec12	Channels B, C, D and E	**Integrity protection.** Patient data shall be integrity protected when transmitted across open networks.
Sec13	Central system	**Data integrity verification.** Central system shall verify the integrity of patient data.
Sec14	Central system	**Data origin authentication.** Central system shall authenticate the Patient data collector (integrity and accountability)
Sec15	Central system	**No unauthorized access**. Central system shall not give unauthorised actors any type of access (view, insert, transform, delete) to patient data in the central system (confidentiality and integrity)
Sec16	Central system	**Patient identity.** Central system shall know the identity of the patient to whom the patient data pertains (integrity)
Sec17	Central system	**Source type.** Central system shall know the type of Source used to produce the patient data (integrity)
Sec18	Channel D	**Authenticate User.** Central system shall authenticate the User (confidentiality and accountability)

[1] "Integrity verification" refers to the verification that data has not been altered during transmission from the Source; it does not imply a "sanity check" on the data. Such a sanity check should be implemented somewhere in the system, at least in the Central system before storage of the data.

No.	*Actor(s)*	*Requirement*
Sec19	Channel D	**Authenticate Central System.** Patient data consumer shall authenticate the Central system (integrity)
Sec20	Channel E	**Authenticate User.** Patient data collector shall authenticate the User (confidentiality and accountability)
Sec21	Channel E	**Authenticate Patient data collector.** Patient data consumer shall authenticate the Patient data collector (integrity)
Sec22	Patient data consumer	**Data integrity verification.** Patient data consumer shall verify the integrity of patient data
Sec23	Patient data consumer	**No unauthorized access.** Patient data consumer shall not give unauthorised actors any type of access (view, insert, transform, delete) to patient data from the Patient data consumer (confidentiality and integrity)
Sec24	All components	**Emergency access.** Where emergency access functionality is available, invocation of emergency access shall override any restriction on read access (availability)
Sec25	All components except Source	**Emergency access monitoring**. Emergency access shall trigger extended monitoring of relevant events to enable detection of unnecessary access (confidentiality and accountability)

Note: Not all requirements can or should be fulfilled by technological security measures implemented in the system. Some requirements may e.g. be fulfilled through human procedures or physical security measures outside of the system, such as physical access barriers for entering an operation room.

2.6 Requirements Derived from Other Requirements

No.	*Actor(s)*	*Requirement*	*Explanation*
Derived1	Patient data collector	**Trusted entity.** Patient data collector should be trusted to handle unencrypted patient data.	Follows from the Sources' lacking capabilities to create end-to-end secure channels to Patient data receivers.

No.	*Actor(s)*	*Requirement*	*Explanation*
Derived2	Patient data forwarder	**Not trusted entity.** Patient data forwarder should not be trusted to handle unencrypted patient data.	The number of trusted entities should always be kept to a minimum, and the Patient data collector should be able to manage end-to-end security with the Central system or Patient data consumer.