Privacy Requirements for Low-Cost Chronomedical Systems

Christopher Adams

Abstract

The Phoenix Ambulatory Blood Pressure Monitoring System is conceived around an inexpensive, unobtrusive, and easy-to-use device that is worn by a person to collect a week of blood pressure measurements. The system includes two software components: one that creates a sphygmochron from data collected with the device for a single person during a single study span, and another component for modeling blood pressure patterns in whole populations. The Phoenix System is intended for a variety of scenarios that include self-care, clinical care, public health, and research. These scenarios impose personal and legal demands for privacy that the system meets by relegating any burden of privacy to a caregiver while minimizing the constraints posed by system on the caregiver's process. Rather than building functionality to comply with privacy constraints, the goal is to unburden the system of privacy issues. These goals are expressed through a surprisingly short list of simple requirements.

Key Concepts

Anonymity	is a quality or state of being unknown or unacknowledged
Privacy	is a state of being free from unsanctioned intrusion
Security	is a condition of not being threatened, especially physically, psychologically, emotionally, or financially

Principles

Though not necessarily universal, some principles are certainly drivers in significant medical device markets:

- Privacy is power
- The wearer of a device owns data from the device, which are measurements of the wearer's body
- Caregivers are custodians
- Control belongs to the wearer

Legal Constraints

These principles are reinforced by, if not expressly codified in, various regulations.

In the United States, individual privacy is a constitutional right. The dominant legislative protection of medical privacy is the Health Insurance Portability and Accountability Act of 1996, HIPAA. HIPAA was instigated by a need to reduce the cost of healthcare. It is primarily about healthcare insurance and the privacy of data that accompanies insurance claims. Though the act does not cover all healthcare activities, the scope is broad enough to affect most healthcare providers in the country, as well as healthcare technology and service companies. [1]

In the United States, privacy is also regulated at the state level.

In Europe, privacy is based on individual rights that are encoded in a variety of instruments:

- Treaty – such as the European Convention of Human Rights
- Legislation – such as the United Kingdom's Data Protection Act (DPA)
- Constitution – such as France's Declaration of the Rights of Man and of the Citizen

In Europe, it is generally not legal to grant access to medical information on a need-to-know basis. In Europe, the patient must expressly grant access.

Context — System Architecture and Usage Scenarios

Medical devices are used in contexts where privacy is important. The principles and regulatory constraints described above highlight why privacy is important. The following scenarios highlight where those privacy concerns must influence the design.

Conceptual Architecture

The Phoenix Ambulatory Blood Pressure Monitoring System is conceived around an inexpensive, unobtrusive, and easy-to-use device that is worn by a person to collect a week of blood pressure measurements. The system includes two software components: one that creates a sphygmochron from data collected with the device for a single person during a single study span, and another component for modeling blood pressure patterns in whole populations. The models in the session analysis software rely on parameters derived with the reference data software, which in turn depends on data collected from as many sessions as can be obtained by the physiologist. The sphygmochron provides the wearer with a chronobiologic assessment of blood pressure and hear rate.

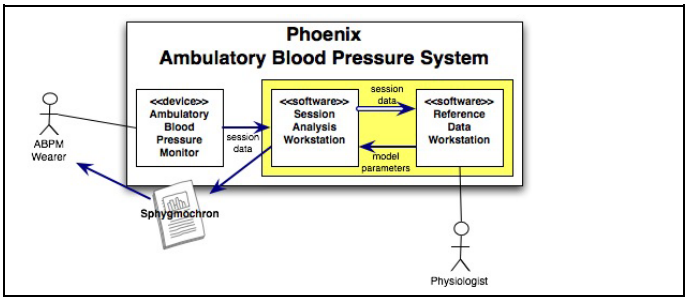

Figure 1. Phoenix Architecture

Scenario 1 – Home-Based Self-Care

Here is a story from a hypothetical wearer of the Phoenix ambulatory blood pressure monitor:

> I'm basically a healthy person, but as I grow older, I am concerned that my blood pressure might be too high when I exercise. I visit a sports clinic and, as I expected, the clinicians take some preliminary measurements, take my history, and listen to my concerns. They suggest a continuous blood pressure monitor. That sounds much better than trying to capture the readings at intervals when I am in a pattern that I don't wish to interrupt every few minutes, and particularly if I am playing a match, such as squash. The clinicians also discuss the importance of keeping track of activities and events in a journal or log. They want me to keep track of things outside a "usual" day, such as playing squash, working with weights, jogging, etc., as well as events that happen to me, like accidents, personal conflicts, etc. [3]
>
> From the clinic, a neighborhood pharmacy, or an Internet-based supply company, I obtain a personal monitor, analysis software, and a cable that connects the monitor to my personal computer. I install the software on my computer and incorporate blood pressure monitoring into my regular exercise routine.

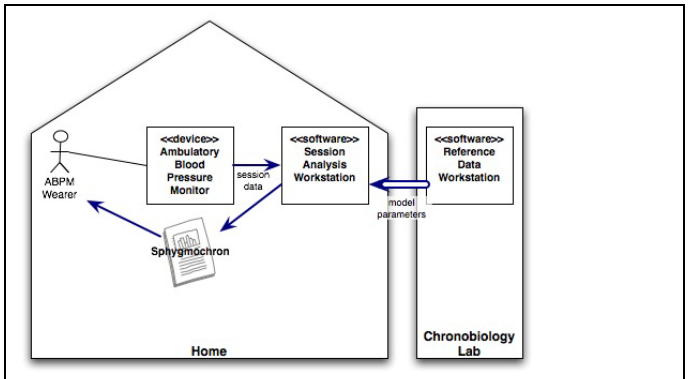

Figure 2. Home-Based Self-Care Scenario

In this scenario, all monitoring and analysis takes place in the wearer's home. The wearer may download software updates from a resource on the Internet, but no data flows in the opposite direction. Because data is not exposed to anyone other than the wearer, there are no potential threats to privacy.

Scenario 2 – Internet-Based, Individual Health Surveillance

This scenario is similar to the home-based self-care scenario, except that special software on the wearer's computer is not used. Rather, the device is designed so that when it is connected to the wearer's computer, the device's data is presented as a simple file that can be uploaded to a Web site that automatically analyzes the data and generates a report that is then returned to the wearer's computer, perhaps as a PDF file.

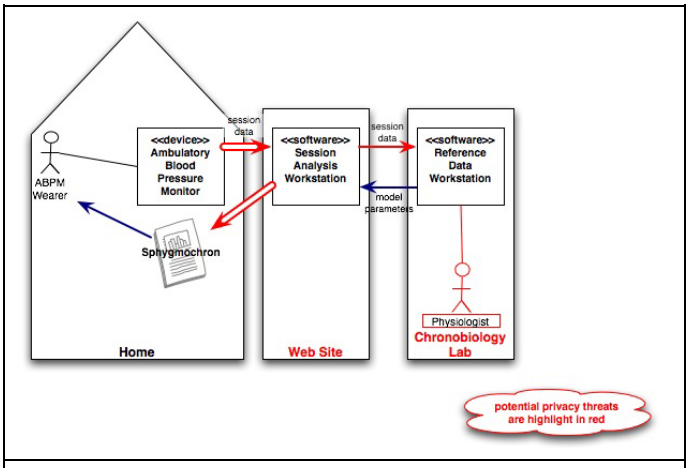

Figure 3. Individual Health Surveillance Scenario

The difference between this scenario and the home-based scenario is the exposure of the wearer's data to physiologists who maintain the Web site and use the data to model population profiles, which are then fed back into the analysis software.

Scenario 3 – Clinical Care

In this scenario, clinicians use the system to monitor a patient and diagnose disease.

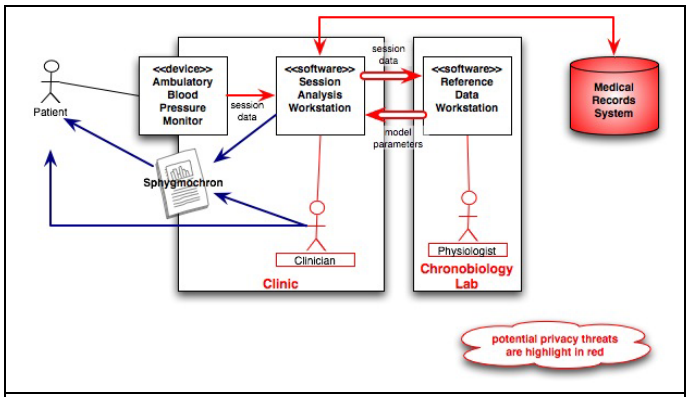

Figure 4. Clinical Care Scenario

Here is an abbreviated scenario for an outpatient clinical encounter. [5]

1. The "encounter" – clinician meets with patient for medical history, physical exam, counseling, review of older chart data, etc.
2. Clinician assesses the patient and plans treatment.
3. Clinician records information about encounter in the clinical chart.
4. Tests are performed by clinic staff (lab specimen collection, radiology, etc).
5. Clinician meets again with the patient to review, report and discuss the results of the "tests".
6. Clinician revises the assessment and plan.
7. Patient is given recommendations for follow-up (e.g., prescriptions or referrals)
8. Patient makes a follow-up appointment as needed.

During an initial appointment, preliminary readings may be taken during the test step (4) and a device prescribed and given to the patient, along with counseling, during the recommendation step (7). In a follow-up exam, session data may be collected during the encounter (step 1) or during the test step (4).

Scenario 4 – Self-Care Followed by Clinical Care

A natural scenario is one where a person using the device for self-care (scenario 2) detects or perceives an abnormality based on feedback from the system, and then takes the matter to a clinic (scenario 3) for follow-up. The patient will want to bring the self-collected data and reports into the clinic, for consideration along with, and inclusion into, the medical history. The clinician will want to analyze a series of sessions, some collected during self-care and others under the prescription of the clinician.

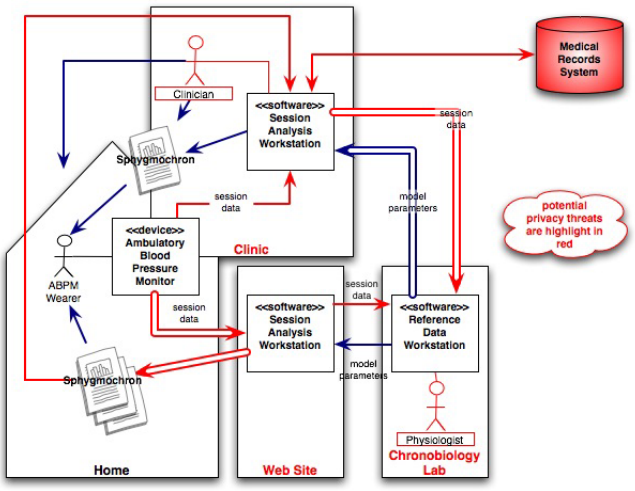

Figure 5. Combined Scenario

Scenario 5 – Public Healthcare

Public health is concerned with threats to the overall health of a community based on population health analysis. It is feasible that public healthcare introduce widespread surveillance to not only improve the individual healthcare provided by the healthcare agency, but also to shift the entire population from after-the-fact care to prevention that reduces widespread morbidity and mortality.

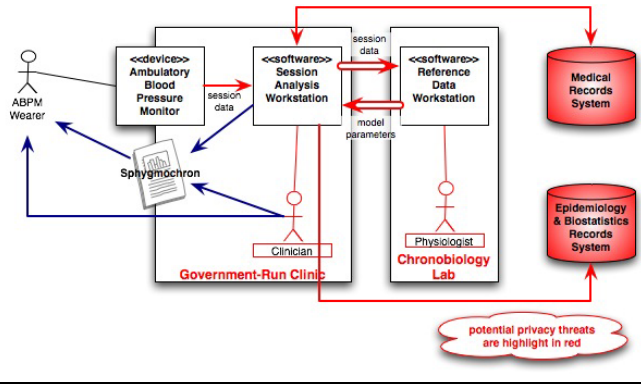

Figure 6. Public Healthcare Scenario

Public healthcare involves extensive epidemiology and biostatistics, which means a lot of data is collected. Public healthcare is usually a function of government, though nongovernmental organizations sometimes serve as public health agencies. This means that the data is accessible to large numbers of people with whom many would be reluctant to share personal details. The intent is not to stop the sharing but to control it.

Health services are frequently a major component of public healthcare. Therefore, as shown in Figure 6, a significant part of the public healthcare scenario flows like the clinical-care scenario (3). Also, public health policy often stresses education in combination with self-care, so a public healthcare scenario might emulate the home-based self-care scenario (1), the Internet-based self-surveillance scenario (2), or the combination of self-care and clinical care (4).

Scenario 6 – Research

The research scenario [2] follows this general process:

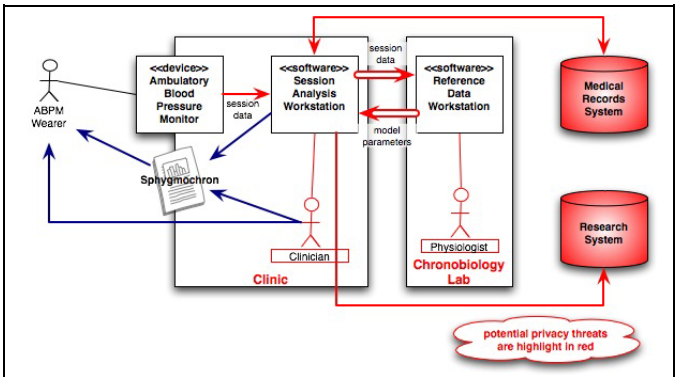

Figure 7. Research Scenario

1. Research Project Initiation
   - Major research organization obtains funding for the research on the preventive effects of blood pressure monitoring
   - Detailed test schedule is developed
   - Volunteer candidates are invited through newspapers or Internet
   - Current patients can be also invited if they are within the test scope
   - Doctors, nurses and technicians are instructed on the details of the particular test
2. Candidate Selection
   - Scientists and Doctors are major players during the test selection, insuring proper initial condition of the test. Condition of the patient is documented at this point
   - Lawyer is hired by the research organization to insure proper legal framework of the process
3. Preparation
   - Selected participants are instructed by nurse and technician about how to use the monitor
   - Placebo monitors can be considered to insure accuracy
   - Participants wear the monitor for some time (maybe a week) to get used to it
4. Test
   - The length of the test is determined by the scientists
   - During the test, participants provide their data and diaries weekly to the scientists, using secure dedicated internet connection
   - Doctors monitor the condition of the patients regularly
   - Drop-outs can stop their participation at any time and return the monitor
5. Results analysis
   - After the conclusion of the test, researchers analyze the results using statistical methods according to their project plan
   - Participants can get the information on their pressure patterns, along with the doctor's analysis and advice

This scenario has most of the privacy weaknesses of the public healthcare scenario (5). In the research scenario, corporate entities and not just government bodies may have access to the medical data.

Design Goals

The Phoenix Project is chartered as an open-source endeavor. As such, the project is organized around self-organizing teams, in which individuals take on roles by volunteering for specific tasks. Open-source medical devices are rare; the effort is challenging, both technically and organizationally. To improve the chances of success, the architects adopted the following goals for the design:

- Unburden Phoenix of privacy issues
- Relegate the burden of privacy to caregivers
- Minimize the constraints posed by Phoenix on a caregiver's process

System Requirements

The privacy requirements are surprisingly simple:

- Group data by session, where a session is a period (nominally a week) during which data is continuously collected from a wearer with a given device
- Identify a session by a session key
- Primarily identify collected data by the session key
- Make the session key available to external systems

- Trace each session to the device employed in the session
- Manage person (patient) identity externally
- Within the system, keep all data anonymous
- Include anonymous fields in reports/displays
  - Anonymous fields are intended for person identity but can be repurposed
  - Anonymous fields may be ignored
- Assign labels and values to anonymous fields from an external source

These requirements are not specific to the Phoenix blood pressure monitor. They could easily apply to many monitoring devices.

References

[1] Adams, Christopher. "About HIPAA."

[2] Khodak, Andrei. "Research Scenario." Phoenix Project, internal project document.

[3] Leinke, Dennis. "Self-Care Scenario." Phoenix Project, internal project document.

[4] Phoenix Project, Twin Cities Chapter of IEEE, Halberg Chronobiology Center. http://www.phoenix.tc-ieee.org/. Project home page.

[5] Werth, Dr. Gerald R., MD PhD MSEE. "Clinical Care Scenario." Phoenix Project, internal project document.