

Spring 2011

# Impediment sensitive-role based access control

Joseph Frederick Blumberg  
*James Madison University*

Follow this and additional works at: <https://commons.lib.jmu.edu/master201019>



Part of the [Computer Sciences Commons](#)

---

## Recommended Citation

Blumberg, Joseph Frederick, "Impediment sensitive-role based access control" (2011). *Masters Theses*. 154.  
<https://commons.lib.jmu.edu/master201019/154>

This Thesis is brought to you for free and open access by the The Graduate School at JMU Scholarly Commons. It has been accepted for inclusion in Masters Theses by an authorized administrator of JMU Scholarly Commons. For more information, please contact [dc\\_admin@jmu.edu](mailto:dc_admin@jmu.edu).

Impediment Sensitive - Role Based Access Control

Joseph Frederick Blumberg

A thesis submitted to the Graduate Faculty of

JAMES MADISON UNIVERSITY

In

Partial Fulfillment of the Requirements

for the degree of

Master of Science

Computer Science

April 2011

## Dedication

This thesis is dedicated to Sandra, my wife and soul mate, and to everyone who stood with me in times of crisis and joy.

## Acknowledgements

I would like to extend sincere gratitude to my committee chair Dr. M. Hossain Heydari and my committee members Dr. John McDermott and Dr. Brent Tjaden for their time, patience, insights, and wisdom.

## Table of Contents

List of Tables .....	vi
List of Figures .....	vii
Abstract .....	viii
1 Introduction.....	1
2 Background .....	3
2.1 Systems .....	3
2.2 Instruments.....	5
2.2.1 Insulin Pump .....	5
2.2.2 Pacemaker .....	7
2.2.3 Instant Heart Rate Application.....	10
2.3 Failure .....	11
2.3.1 Definitions.....	11
2.3.2 Instrument Failure.....	18
2.3.2.1 Instrument Failure Impacts .....	20
2.3.2.1.1 Low Battery .....	21
2.3.2.1.2 Lost Wireless Signal .....	23
2.3.2.1.3 Broken Connector .....	24
2.3.2.1.4 Clogged Tube.....	25
2.3.2.1.5 Low Medicine/Solutions .....	25
2.3.3 User Failure.....	26
2.3.3.1 User Failure Impacts .....	27
2.3.3.1.1 Mental States.....	28
2.3.3.1.2 Lacerations and Fractures .....	29
2.3.3.1.3 Death .....	29
2.4 Environmental Situations.....	30
2.4.1 Hospital Code Red .....	32
2.4.2 Airplane Mode .....	32
2.4.3 Displaced.....	33
2.5 Data Availability and User role assignments.....	33
2.5.1 Data Availability .....	35
2.5.2 User Role Assignments.....	35
2.6 RBAC .....	36
2.6.1 Basic RBAC.....	36
2.6.2 Context Sensitive .....	36
2.6.3 GeoTemporal .....	37
2.6.4 Fuzzy RBAC.....	37
2.6.5 Privacy Sensitive RBAC.....	38
2.6.6 Adding Attributes.....	40
3 Impediment Sensitive - RBAC Model.....	41
3.1 IS -RBAC Definitions.....	43
3.2 IS-RBAC Example.....	48

3.2.1	IS-RBAC Example Description .....	49
3.2.2	Unanticipated Role Accesses .....	49
3.2.3	Authorized Role Accesses .....	52
3.2.4	Role Re-assignments.....	56
3.2.4.1	Assignment to the Patient Role.....	56
3.2.4.2	Assignment to the Web Server Global Support Role.....	56
3.2.4.3	Assignment to the Physician’s Assistant Role.....	57
3.2.4.4	Assignment to the Nurse Role .....	57
3.2.5	Threat Mitigation .....	57
3.2.6	IS-RBAC Example Definitions.....	58
3.3	Summary .....	71
4	Conclusions.....	73
5	Future work.....	75
6	Appendix A: Additional Embedded or Closely Worn Medical Devices .....	77
6.1	Insulin Pump: CareLink Website.....	77
6.2	Pacemaker.....	79
6.3	Hearing Aid.....	79
6.4	H’andy Sana 210.....	83
6.5	ICE: In Case of Emergency Application.....	84
6.6	Heart Rate Monitor .....	85
6.7	ICE Medical ID Card .....	89
6.8	Cardio Trainer.....	91
6.9	Electric “Sheep”.....	92
6.10	Ultrasound.....	94
7	Appendix B: ICD10 .....	95
8	Appendix C: Siemens Hearing Instruments - Troubleshooting .....	98
	Bibliography .....	100

## List of Tables

Table 1. Instrument failures and their impacts to user role assignments and data availability. ....	21
Table 2. User failures and their impacts to user role assignments and data availability.....	27
Table 3. Environmental situations and their impacts to user role assignments and data availability. ....	31
Table 4. Expected and unforeseen access to patient PII located on the insulin pump. ....	51
Table 5. Expected and unforeseen access to patient PII, located on the web server.....	52
Table 6. Authorized IS-RBACs to patient PII located on the insulin pump. ....	53
Table 7. Authorized IS-RBACs to patient PII located on the Web Server. ....	54
Table 8. Data sensitivities to instrument failures. ....	61
Table 9. Data sensitivities to user failure. ....	61
Table 10. Data sensitivities to Impediments. ....	62
Table 11. IDP: Data sensitivities to Impediments and associated permissions; per data souce....	64
Table 12. User role assignments with sensitivity to user failure.....	66
Table 13. User role assignments with sensitivity to instrument failure. ....	67
Table 14. User role assignments sensitive to environmental situation. ....	68
Table 15. Impediment sensitive user role assignments. ....	69
Table 16. Impediment free session. ....	70
Table 17. Clogged tube on the insulin pump session.....	71

## List of Figures

Figure 1. The Medtronic Guardian REAL-time insulin pump.....	5
Figure 2. The Medtronic CareLink Network pacemaker remote monitoring system. ....	8
Figure 3. The Biotronik pacemaker Home Monitoring system. ....	8
Figure 4. Reduction of the patient heart rate variability. ....	9
Figure 5. Instant Heart Rate smartphone application.....	10
Figure 6. Twitter feed of users’ heart rates. ....	11
Figure 7. Laprie’s dependability model. Sommerville used “Impediments” instead of “Threats”. .....	13
Figure 8. Avizienis’ and Laprie’s, et al., “elementary” fault classes. ....	14
Figure 9. A refined dependability and security tree.....	15
Figure 10. A receiver unit properly connected to the hearing aid base.....	19
Figure 11. A broken receiver unit connection pin on the hearing aid base.....	19
Figure 12. User information (e.g., PII) on the CareLink website. ....	77
Figure 13. Logbook entry on the CareLink website. ....	78
Figure 14. PII and medical information on the CareLink website. ....	78
Figure 15. A pacemaker placement.....	79
Figure 16. Siemens Pure hearing aid. ....	80
Figure 17. Siemens Pure hearing aid with Bluetooth remote control. ....	80
Figure 18. Siemes Pure hearing aid with pocket remote control. ....	81
Figure 19. The H’andy Sana 210 with “Heart Suite” ECG phone.....	83
Figure 20. The H’andy Sana 210. Placing fingers on the sensors.....	84
Figure 21. Sample ICE screen shots. ....	85
Figure 22. The HxM™ BT module (device with Zepher written on it) and the Zephyr Bioharness for monitoring a person’s heart rate, speed, and distance. ....	86
Figure 23. The SportTrackLive application on an Android smartphone. ....	87
Figure 24. Live user monitoring data uploaded to shared website <a href="http://www.sportstracklive.com/">http://www.sportstracklive.com/</a> .....	87
Figure 25. Detailed information from Live user monitoring. ....	88
Figure 26. Detailed location from Live user monitoring. ....	88
Figure 27. ICE Medical ID card. A USB thumb drive in a credit card format. ....	90
Figure 28. Pop-out the thumb drive and insert into USB port of computer.....	90
Figure 29. Screen capture of ICE Medical ID application.....	90
Figure 30. Cardio Trainer application on Android smartphone.....	91
Figure 31. Cardio Trainer exercise activity uploaded and displayed on John Smith’s Google Health website.....	92
Figure 32. Movement levels detected by Electric Sheep application on Android smartphone. ...	93
Figure 33. The VSCAN handheld ultrasound.....	94



## Abstract

This paper introduces a variation to the Role Based Access Control (RBAC) model called Impediment Sensitive RBAC (IS-RBAC) to be used for implantable and closely-worn medical devices. The IS-RBAC represents impediments including instrument failures, user failures, and environmental situations. IS-RBAC accommodates the impacts that the three types of impediments convey on two foundation set definitions, namely, the data set and the set of user role assignments. With these new definitions, IS-RBAC model strengthens the weaknesses caused to the protection of data from user and instrument failures and environmental situations, mitigates threats from users with elevated user role privileges, and ultimately helps prevent potential harm to data owners. Implantable and closely worn medical devices (instruments) offer substantial examples to illustrate applicability of the IS-RBAC model. This paper presents instrument and user failures and environmental situations associated with instrument Socio-Technical Systems including a modern heart pacemaker, insulin pump, hearing aid, and several smartphone sensory applications.

# 1 Introduction

Advances in technologies offer the medical community a multitude of new information sources, storage locations, and analytical opportunities to improve patient health care. These same advances in technologies offer opportunities for additional conditions under which information may be accessed in an unauthorized, undesired, or unanticipated fashion. Medical systems fail in a variety of ways under many circumstances. Patients' biological states also present an even wider range of situations in which Personally Identifiable Information (PII) may be required by doctors, medical staff, emergency medical technicians, and even good Samaritans. Additionally, HIPAA [1] stipulates restrictive "...standards and requirements for the electronic transmission of certain health information."

In combination, the convergence (ubiquity) of technology, the failing states of computer instruments, the diverse information needs by an assortment of medical actors, and the environmental situations in which the systems and users must operate, offer a difficult environment to prepare a secure system. While there are many solutions to protect the confidentiality and integrity of medical PII in relatively static computing environments, few research efforts address situations where distinct instrument and user failure states and environmental situations formally impede the application of different confidentiality directives. Some research efforts examine "privacy-aware" Role-Based Access Controls (RBACs)[2] and "context constraints in RBAC environments." [3] However, these research efforts consider RBACs based on the nature or "purpose" [4] of the information.

This thesis employs Summerville's [5] concept that computer technologies and their respective users interlock into a structure called a Socio-Technical System. The contributions of this thesis include the following for Socio-Technical Systems:

- 1) Identify instrument and user failings and environmental situations as impediments to user role assignments and data availability in Socio-Technical Systems.
- 2) Identify a taxonomy that classifies instrument failures and an internationally accepted taxonomy that classifies user failures.
- 3) Develop a variation of the role-based access control (RBAC) model. This new model, termed an Impediment Sensitive Role-Based Access Control (IS-RBAC), represents the sensitivities to data availability and user role assignments that instrument and user failures and environmental situations have on Socio-Technical Systems.
- 4) Apply the IS-RBAC model to an example Socio-Technical System consisting of an insulin pump, web server, patient, PII, and a variety of additional user roles.

This thesis is organized into 4 additional sections and a few appendices. The next section presents background information about Socio-Technical Systems, few example Socio-Technical Systems found in the medical arena, an overview of failures and their impediment to Socio-Technical Systems, and a review of RBAC models. After the background section, the IS-RBAC model is introduced, defined, and illustrated from an example of a Socio-Technical System. The latter two sections present conclusions and future work suggestions.

## 2 Background

This section begins with a review of systems, namely Technical Computer-Based Systems and Socio-Technical Systems. The background continues with a discussion of medical instruments, their failures and for lack of a better term, user failures. The medical instruments used are closely worn by or embedded in the patient. Non-medical components such as a smartphone, desktop computer, and a web server, comprise the overall Socio-Technical System and work in conjunction with these medical instruments. The failures in these Socio-Technical Systems are shown to impact access controls to, and at times, information. Also presented are few medical environmental situations which also impact access controls. The nature of the instruments discuss provides insights into the fashion in which the instrument and user failures and environmental situations affect access controls. Lastly, this section presents a review of RBAC models.

### 2.1 Systems

Sommerville [5] describes two categories of software systems, namely, Technical Computer-Based Systems and Socio-Technical Systems.

Technical Computer-Based Systems are systems that include hardware and software components but not procedures and processes.

Socio-Technical Systems include one or more Technical Computer-Based Systems but, crucially, also include knowledge of how the system should be used to achieve some broader objective.

Dewsbury[6] describes the role of the user and surmises their impact on dependability of home based domestic systems. This could not be any truer for instruments (the ultimate domestic systems) presented in this paper.

Most dependability theory attempts to consider humans as elements in the system that are comparable with other software or hardware elements.

For domestic systems, the users of the system are central to the design and central to the consideration of dependability. In the home, there are no defined operational processes, enormous variation in system users, and no “quality control”. The dependability of home systems is played out daily through the routines and situated actions of the people in the home.

Malicious attacks or inadvertent unauthorized access to PII can occur at many places in a Socio-Technical System. For example, in systems which include a centralized database located at a company’s facility, administration personnel at the facility may have physical access to data in an unauthorized fashion. Likewise, in a system in which data traverses the Internet, unauthorized users may attack data at edge routers.

Internet based systems allow PII to be shared in an unprotected fashion. The information in the system can be shared with other outside systems via human interactions such as an email or a scan of hardcopy data. Systems with wireless technologies such as Wi-Fi and Bluetooth may be subject to intercept, either nefariously or accidentally. They are also subject to a denial of service if located in a noisy electromagnetic environment or if switched to Airplane mode as in the case of a smartphone on an airplane.

Physical access to a user’s smartphone may allow an actor to gain unauthorized access to PII. Similarly, physical access to almost any computer server or workstation component of the system may yield the same unauthorized access.

To summarize, Socio-Technical Systems inherit the same INFOSEC properties (Confidentiality, Integrity, and Availability) as the individual Technical Computer-Based Systems which make up the total system. The INFOSEC properties of system components not only include the hardware and software, but also include the INFOSEC properties associated with people (users, operators, technicians, administrators). The access control model should take this in account by representing changes to data availability, user role assignments, and environmental situations of Socio-Technical Systems.

## 2.2 Instruments

This section presents a variety of Socio-Technical Systems found in the medical arena. Each consists of Technical Computer-Based Systems and users. At least one of the Technical Computer-Based Systems is a closely worn or implantable medical instrument. A variety of technologies connect them to other elements in the Socio-Technical Systems including wireless networks, Bluetooth, or Internet. Users include the patient, physician, and technical close support personnel.

In order to provide brevity here, only three Socio-Technical Systems are presented in this section and the remaining are described in Appendix A.

### 2.2.1 Insulin Pump

The Medtronic Guardian REAL-time insulin pump [7] shown in Figure 1 offers advanced monitoring and infusion of insulin.



Figure 1. The Medtronic Guardian REAL-time insulin pump.

This instrument can interface with personal computers for the user and physician via Medtronic's CareLink software[8], either the personal or professional version. The personal version of the software is described on the Medtronic [8] website as follows:

CareLink™ Personal is software designed for Patients and is run via a website. This secure, online therapy management software downloads data from your pump to turn into reports, giving you superior insight into patterns of your diabetes and therapy. As long as you have a CareLink USB with you, you can download your pump data at home or

anywhere that you have Internet access. Just like a web email account, you just register and login.

This system has several Technical Computer-Based Systems and users which interact together to compose a Socio-Technical System. The Socio-Technical System includes the pump shown in Figure 1, the website (computer and software system) to which the user's data will be uploaded, and the CareLink™ Personal software with its components as listed below (per Medtronic's web site[9]).

- Access to a computer running Windows® 98SE, ME, 2000, XP, or Vista 32 bit.
- A reliable Internet connection
- Microsoft® Internet Explorer version 5.5 or higher, Adobe® Reader™ version 5.0 or higher
- A CareLink™ USB connectivity device (provided with your Paradigm Veo insulin pump)
- A Blood Glucose Monitor with an appropriate cable if you would like to download this into CareLink Personal separately.

The users and other actors who own a part in this Socio-Technical System include the user of the pump (the patient), the administrators of the user's Internet Service Provider, the administrators of the Internet server and CareLink website, and the additional consumers of the user's information such as the nurses, doctors, and administrators of the doctor's computer systems. The type of information stored in the CareLink website is provided in Appendix A.

According to Medtronic, "The system also uses Secure Sockets Layer (SSL), a data encryption technology, which ensures that data is unreadable during the transfer." Thus, an individual on the Internet would be required to crack the SSL session if trying to capture user data in an unauthorized fashion.

The environments in which the insulin pump and CareLink computing systems operate are as varied as users' imaginations. Today's PCs are quite mobile, small, portable, and powerful. With a cellular based ISP, the insulin pump and PC components can be connected to

the Internet and the CareLink website from virtually anywhere in the world under all types of environmental conditions. Some of these environments for consideration include automobiles on our highways, hotels, hospitals, parks, etc. In these different physical environments, some adverse conditions may influence the Socio-Technical System such as an automobile accident in which the user is injured, hospital coded conditions, and Internet connection dropouts in remote areas of parks.

### **2.2.2 Pacemaker**

According to the Mayo Clinic [10], “a pacemaker is a small device, about the size of a pocket watch, that's placed under the skin near your heart to help control your heartbeat. People may need a pacemaker for a variety of reasons — mostly due to one of a group of conditions called arrhythmias, in which the heart's rhythm is abnormal.” Appendix A depicts placement of a pacemaker in the body.

The Medtronic CareLink Network pacemaker remote monitoring system depicted in Figure 2 “ensures timely identification of clinically important issues, such as asymptomatic atrial fibrillation or device integrity issues.”[11] The Medtronic CareLink Network device provides the user with critical device conditions including the following [11]:

- Full parameter summary
- Percent pacing
- Real-time and magnet EGM
- Battery voltage and longevity
- A-V conduction histograms
- Arrhythmia summary with Mode Switch duration
- Lead impedance and trends





Figure 2. The Medtronic CareLink Network pacemaker remote monitoring system.

The Biotronik wireless Home Monitoring™ (HM) system provides patients protection during all stages of cardiac resynchronization therapy (CRT)[12]. Figure 3 shows the wireless device attached to a user's waist belt. According to Biotronik's website, the HM system provides the following benefits:

- Early Detection of Atrial Arrhythmias
- Resynchronization Therapy Management
- Lead Monitoring
- ERI Monitoring



Figure 3. The Biotronik pacemaker Home Monitoring system.

An example of Resynchronization Therapy Management [13] (e.g., reduction of patient's hear rate) is shown in Figure 4. The figure shows a trend analysis of uploaded user data. This data provides a trend analysis of PII and might prove embarrassing or politically harmful to the patient if released to unauthorized personnel. The data and analytical products may also contribute to company proprietary analyses or hospital research studies of medications and patient treatments, all of which should be protected like the PII from unauthorized disclosure.

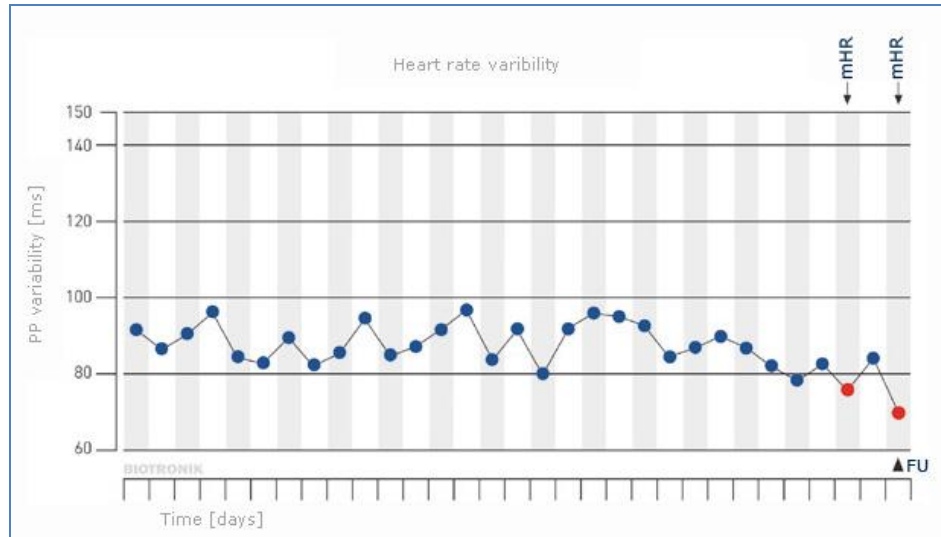


Figure 4. Reduction of the patient heart rate variability.

An advantage of network based monitoring systems is that medical research efforts can analyze data to determine improved medical care. Lazarus [14] analyzes a database of patient pacemaker information gathered from a remote, wireless Home Monitoring™ system (HM). Their objective was to describe “the daily routine application of a new telemonitoring system in a large population of cardiac device recipients.” One of the most notable observations made was that the average amount of time that a patient spends in a visit with a physician when an issue was detected was significantly shortened from regularly scheduled visits. According to Lazarus [14],

The mean interval between last follow-up and occurrence of events notified by HM was 26 days, representing a putative temporal gain of 154 and 64 days in patients usually followed at 6- and 3-month intervals, respectively.

They conclude that such monitoring systems “improve the care of cardiac device recipients, enhance their safety, and optimize the allocation of health resources.”

Access to user information contained in an individual pacemaker device appears controlled; albeit achieved through wireless technologies. However, the environment of this pacemaker Socio-Technical System extends across the Internet to doctors, researchers, and their respective computing systems.

### 2.2.3 Instant Heart Rate Application

Modulo offers a free application on the Android and iPhone smartphones called Instant Heart Rate [15]. It measures a user's heart rate using the built-in camera. The user places their finger over the camera, holds it steady for at least 10 seconds, and then the current heart rate will be shown on the display as shown in Figure 5.

While this device is not imbedded in the user, it is technically closely worn and requires the user to interact with the smartphone device. One could imagine that in the (near) future, the stored information could be sent to doctors, hospitals, and online medical services much in the same way as the H'andy Sana 210 discussed above.

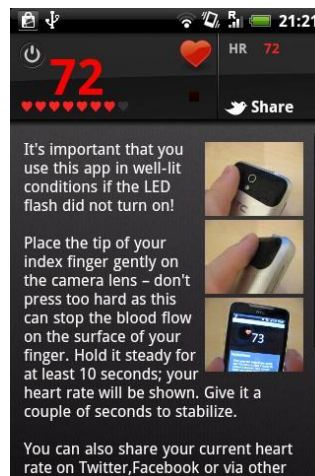


Figure 5. Instant Heart Rate smartphone application.

According to the developers at Modulo [16], “the application has been made as a part of a study that uses sensors built into mobile phones for measuring biological signals.” This study was not described on their website. Thus, the nature, intent, and access controls of additional actors are unknown.

Initially, the environment of the application was limited to the user's smartphone and to this unknown study. We might assume the information was transferred from the smartphones to the study computing environment via the Internet. Additionally, the application saves heart rate

detection events in order to improve performance. The application allows the user to connect to the Internet and display PII (by choice). Specifically, the application can be configured to “tweet” a user’s heart rate. Figure 6 shows a recent twitter feed displayed on Modulo’s web site [17]. On a personal note, this author uses this application but chooses not to tweet results. However, it is unknown if the data is automatically used for the unknown study.

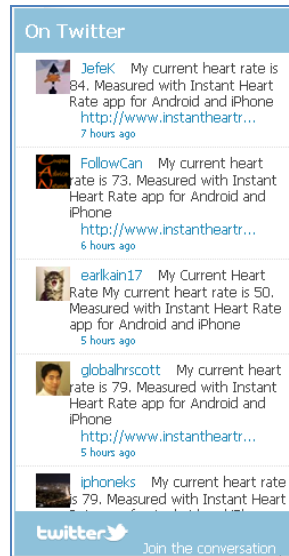


Figure 6. Twitter feed of users’ heart rates.

## 2.3 Failure

The following subsections describe “failure” in the context of instrument and user operations in a Socio-Technical System. The purpose is to define and enumerate how instruments and users fail.

### 2.3.1 Definitions

This section provides a review of general definitions of failure and how failure relates to the dependability and security of a system.

Merriam-Webster [18] defines “failure” as, “a state of inability to perform a normal function.”

Dictionary.com [19] defines “failure” as, “nonperformance of something due, required, or expected: a failure to do what one has promised; a failure to appear.”

The Committee on National Security Systems in the National Information Assurance (IA) Glossary [20] defines the following relevant terms:

fail safe - Automatic protection of programs and/or processing systems when hardware or software failure is detected.

fail soft - Selective termination of affected nonessential processing when hardware or software failure is determined to be imminent.

failover - The capability to switch over automatically (typically without human intervention or warning) to a redundant or standby information system upon the failure or abnormal termination of the previously active system.

failure access - Type of incident in which unauthorized access to data results from hardware or software failure.

failure control - Methodology used to detect imminent hardware or software failure and provide fail safe or fail soft recovery.

Avizienis, Laprie, et al.[21] provide a graphical representation of the taxonomy of attributes for dependable and secure computing as shown in Figure 7, which depicts faults, errors, and failures as a threat to the dependability of a system.

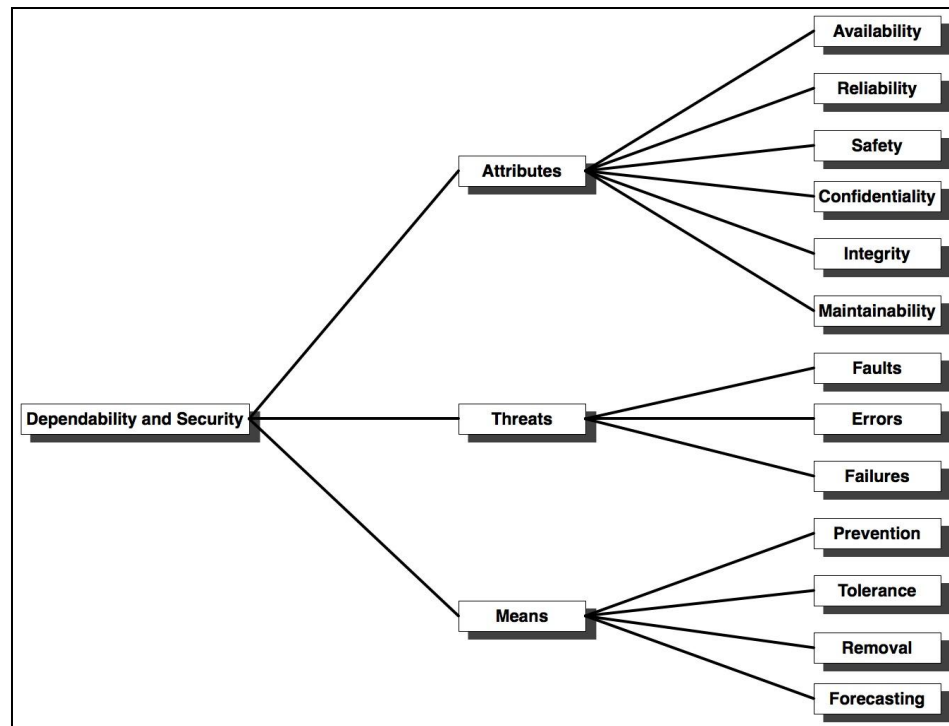


Figure 7. Laprie's dependability model. Sommerville used "Impediments" instead of "Threats".

Dewsbury, Sommerville, et al.[6] use the term "Impairments" instead of "threats" based on an earlier work by Laprie [22]. While faults, errors, and failures are a threat to the dependability of a system, the term threat is quite often used to describe an external client which may violate the security of a system. Bishop [23] defines threat as follows:

A threat is a potential violation of security. The violation need not actually occur for there to be a threat. The fact that the violation might occur means that those actions that could cause it to occur must be guarded against (or prepared for).

While instrument and user failures and environmental situations "threaten" the confidentiality, availability, and integrity of information within a Socio-Technical System, by Bishop's definition failures and situations are not the threat. So, in this paper, we will consider users as the threat or "threat actors"; the term impairments will be used to describe faults, errors, and failures; and the term threat will be used to describe a potential violation of security.

We can say that instrument and user failures and environmental situations weaken a Socio-Technical System for exploitation by threat actors. In order to mitigate these threats, a security model will employ the principle of least privilege as defined by Saltzer [24]. This distinction will be illustrated in the example presented in Section 3.2. Saltzer [25] defines the principle of least privilege as follows:

Every program and every privileged user of the system should operate using the least amount of privilege necessary to complete the job.

Avizienis, Laprie, et al. [26] examine faults in even greater detail and comprised a rather comprehensive taxonomy as shown in Figure 8.

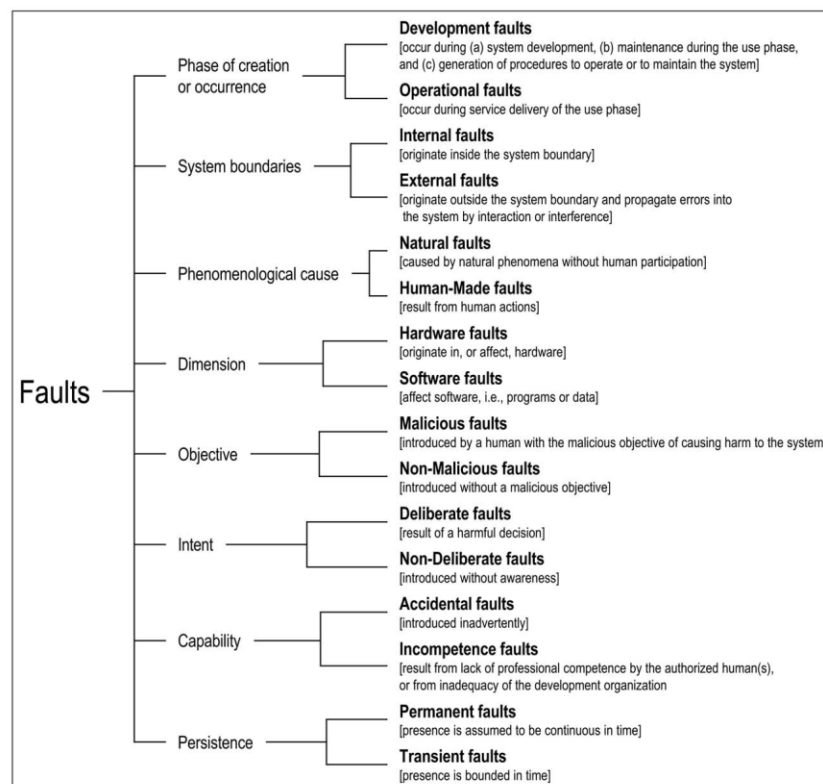


Figure 8. Avizienis' and Laprie's, et al., "elementary" fault classes.

When combined together, the dependability taxonomy in Figure 7 with the elementary fault classes of Figure 8, result in a refined dependability and security tree as shown in Figure 9. However, even with these refinements, the users remain outside the system. According to Laprie [26], users are “entities (humans or other systems) that receive service from the system at their use interfaces.”

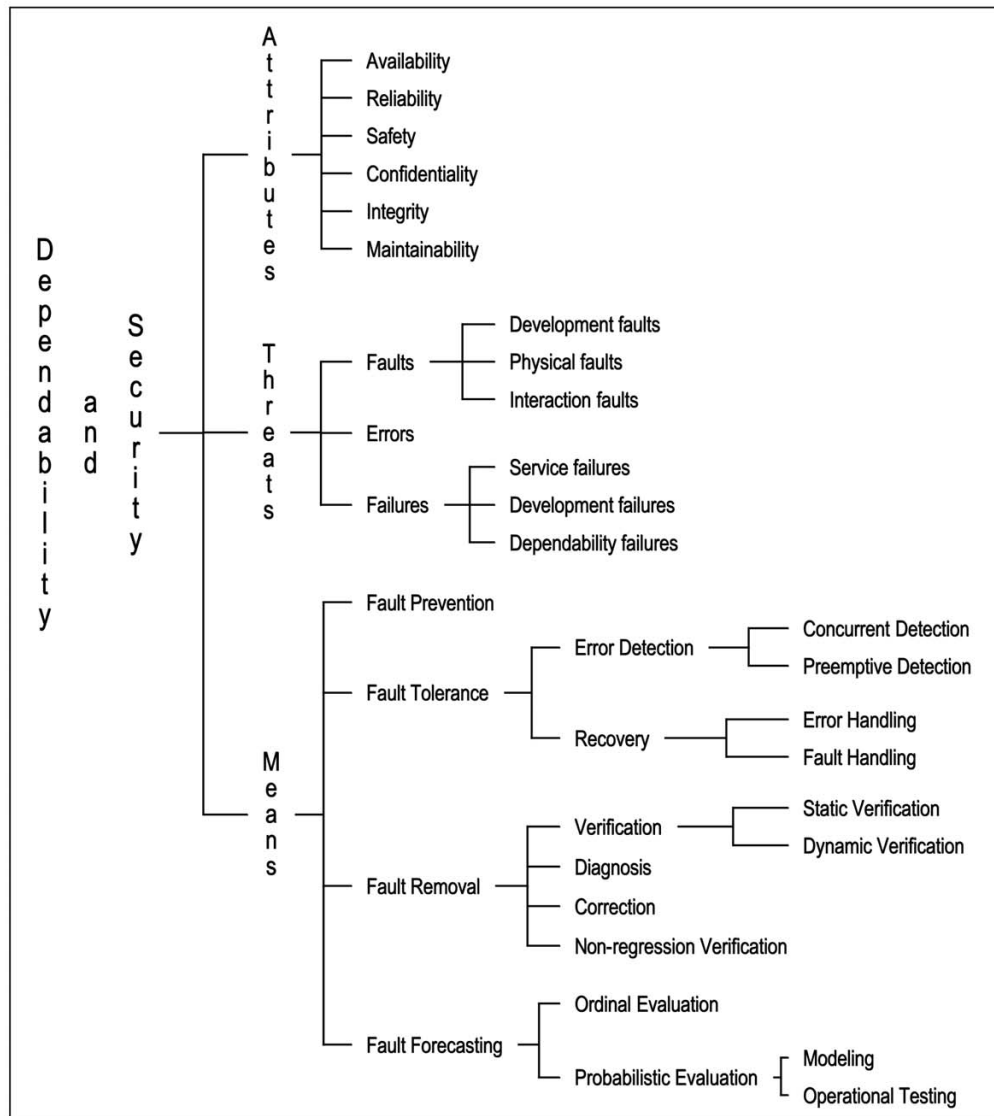


Figure 9. A refined dependability and security tree.



To find out how user faults fit into these dependability taxonomies, we look at a few more definitions of dependability attributes. Sommerville [5] discusses the concept of dependability and four principal dimensions as follows:

**Availability.** Informally, the availability of a system is the probability that it will be up and running and able to deliver useful services at any given time.

**Reliability.** Informally, the reliability of a system is the probability, over a given period of time, that the system will correctly deliver services as expected by the user.

**Safety.** Informally, the safety of a system is a judgment of how likely it is that the system will cause damage to people or its environment.

**Security.** Informally, the security of a system is a judgment of how likely it is that the system can resist accidental or deliberate intrusions.

Sommerville [5] further presents that dependability properties are not applicable to all systems. As an example, he discusses an insulin pump (an example of instrument).

For the insulin pump system, ..., the most important properties are availability (it must work when required), reliability (it must deliver the correct dose of insulin), and safety (it must never deliver a dangerous dose of insulin). Security, in this case, is less likely to be an issue, as the pump will not maintain confidential information and is not networked so cannot be maliciously attacked.

While a probably true statement at the time Sommerville published this example in 2007, technology improvements erode such deductions. Instruments can now store more information and can connect to networks. INFOSEC implications are very real. Information stored in instruments must be protected from unauthorized disclosures (confidentiality). The Medronic Guardian REAL-time insulin pump[27] discussed in Section 2.2.1 offers advanced monitoring and infusion of insulin. The system is also integrated into the user's home network and communicates data to/with medical systems used by health care professionals.

Dewsberry [6] describes Confidentiality and Integrity in terms of home-based and domestic Socio-Technical Systems as follows:

While the need for integrity goes without saying, the issue of confidentiality is much more difficult in situations where elderly people depend on monitoring technology that alerts relatives and carers [care givers] when a problem arises. These elderly users often value their privacy and wish to maintain the confidentiality of their personal information. On the other hand, this may compromise the safety of the overall system as it may limit the speed and type of response in the event of a problem. The level of confidentiality in a system therefore cannot be fixed but has to be programmable and responsive to an analysis of the events being processed by the system.

The last sentence in the description above suggests that the environment in which a Socio-Technical System operates influences confidentiality of information in a variable fashion.

Dewsbury [6] accommodates user interactions with “dependable” home-based (Socio-technical) systems by deriving additional characteristics, namely trustworthiness, acceptability, fitness for purpose, and adaptability. The logic for doing so stemmed from the following assumptions:

People are not automatons and act in unpredictable ways.  
We cannot monitor our brains to identify erroneous states.  
Identifying the fault which resulted in a failure is impossible.

This last assertion, while true, is misleading. For the purpose of a Socio-Technical System, a person’s “fault” is not required. Instead, what is required is just the recognition of a user failure. Thus, when we recognize hardware or processing failures at the boundary of a Technical Computer-Based System we can recognize user failures at the border of the user when that user is considered an integral participant in the operation/function of a Socio-Technical System. And so, identifying a resource that classifies user failures is an important goal of this paper.

Section 2.3.3 describes user failures in terms of the International Classification of Diseases (ICD). The ICD provides a very straight forward, hierarchical, and comprehensive taxonomy of user physiological and psychological conditions.

### 2.3.2 Instrument Failure

The presentation above provides a review of general definitions of failure and how failures generally relate to the dependability and security of a system. This section will highlight instrument failures that dynamically impact data availability and user role assignments. In Section 1, a new access control model is presented that can represent these failures and their changes to data access control protections.

Instruments usually operate under specific physical conditions including temperature, humidity, and/or vibration limitations. Exceeding these limitations may result in component breakdowns and system failures. One aspect of the system may fail leaving other functionalities operational.

One example includes operator error with a partial but critical failure. In this example, the support operator of a hearing aid installs the “receiver unit” (wire that transports signals into the ear) with the hearing aid base. Figure 10 shows the receiver unit properly connected to the hearing aid base. If the receiver unit fails to connect, a connection pin may be broken. Figure 11 shows a broken electrical connection in the hearing aid base. In this example, the hearing aid fails because it is no longer able to deliver a signal externally to the user’s ear but otherwise remains operational. It still retains all information and is still able to connect to a configuration system. However, no procedure is in place to protect the information stored in the hearing aid. As a result, other operators, administrators, and engineers are provided access to user’s PII. While technically these support personnel are authorized to access the PII, users may be unaware of such disclosures. From the instrument perspective, it “Failed open” in that it is still able to communicate with the configuration computer and transmit/receive information.

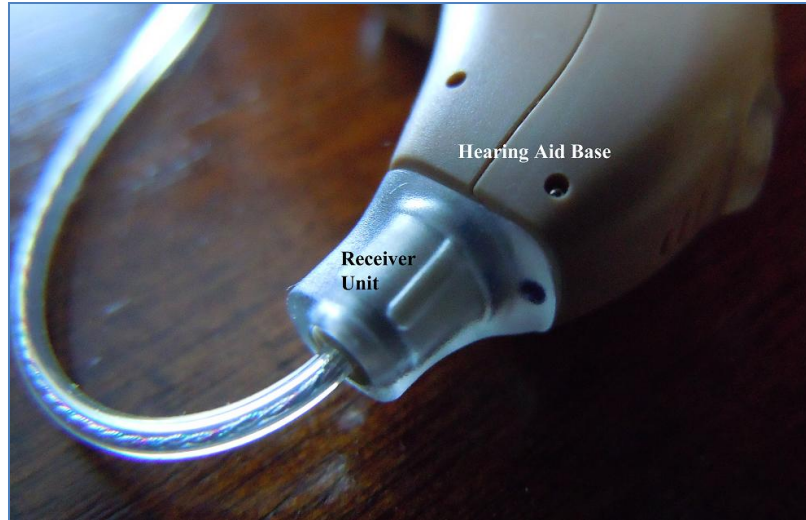


Figure 10. A receiver unit properly connected to the hearing aid base.

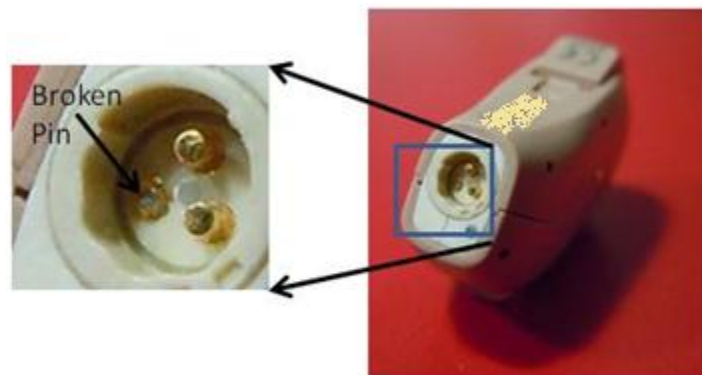


Figure 11. A broken receiver unit connection pin on the hearing aid base.

Another type of failure occurs when a technician or user improperly configures a device. For example, in the previous hearing aid failure, a replacement hearing aid is subsequently used. However, the technician neglects to configure the device. While the device works with preprogrammed default settings, it is not properly synchronized with the other hearing aid nor configured for the user's hearing deficits. One feature of hearing aids is that different listening modes can be selected by the user depending on environmental conditions. However in this example, the devices are not configured and do not synchronize. Thus, when the user selects a different hearing mode, only one of the hearing aids changes modes while the other's operational mode remains unchanged. Thus, the device fault results in the failure to provide the user with

properly synchronized hearing modes of operations. While the devices operate, they failed to operate as expected in total. The devices may or may not detect such synchronization failures but continue to operate in an independent fashion. Thus, the devices do not “fail soft” since there is no termination of function.

Finally, another type of failure occurs with regular expectation. A low battery condition renders a hearing aid partially useful. Its volume slowly decreases until it becomes totally inoperative. During this short period of non-useful but operating condition, a user will seek out new replacement batteries. However, inserting batteries into such a small device requires a relatively high level of fine motion dexterity. Without such a capability a user may introduce additional personnel to assist with this procedure. Physical access to a device may render the information stored within susceptible to unauthorized disclosures.

#### ***2.3.2.1 Instrument Failure Impacts***

Instrument failures impact data availability and user role assignments in the instruments presented in this thesis. Table 1 summarizes these impacts. Further below, each of the five types of instrument failures is presented and the actual or possible changes in data availability and user role assignments are discussed.

Table 1. Instrument failures and their impacts to user role assignments and data availability.

	Low Battery	Lost Wireless Signal	Broken Connector	Clogged Tube	Low Medicine, Solution
Pacemaker	UA, D	UA, D	UA, D	-	-
Insulin Pump	UA, D	UA, D	UA, D	UA, D	UA, D
Hearing Aids	UA, D	UA, D	UA, D	UA, D	-
H'andy Sana 210	D	UA, D	UA, D	-	-
Instant Heart Rate	D	D	D	-	-
Zephyr Heart Rate	D	UA, D	UA, D	-	-
ICE: In Case of Emergency	D	D	D	-	-
ICE Medical ID Card	-	-	UA, D	-	-
Cardio Trainer	D	D	D	-	-
Electric Sheep	D	D	D	-	-
Ultrasound	UA, D	-	D	-	UA, D

UA = User Role Assignment impact

D = Data Availability impact

<dash> = Not Applicable

#### 2.3.2.1.1 Low Battery

While technically not a failure, the Low Battery condition in an instrument allows a user to anticipate a system failure. Inevitably, without recharging or changing the battery, we can assume the system will ultimately fail to operate. During this transition, the user's health may be at grave risk. In this intermediate state between full-power and predestined system shut-down (possibly ending in a disaster for the user), system developers may anticipate proper handling, disposition, and access controls to information contained in the system.

Hypothetically, in order to conserve power a system might be programmed to eliminate certain communication functions, security capabilities, or user information retrieval utilities. System designers may alter the functionality of a system based on power levels in order to maintain the most critical safety functions. For example, in order to maintain a safe condition for the user, the developers of a pacemaker, insulin pump, or hearing aid may disable all communications channels, performance adaptation operations, and maximum strength (volume) settings. The systems may revert to a mode of operation that maintains life and user safety conditions in anticipation of an eventual recharge. Hopefully, the system developers would also have developed a means to notify the user (e.g., hearing aid beeps) of such a condition so that the user can take appropriate actions.

With systems that include a user's cell phone, the users may elect to shut down certain power consuming functions such as Bluetooth, Wi-Fi, cell signal, or GPS. In doing so, the functionality of the system may be adversely affected. Some or all data may not be collected by the system. Data may no longer be uploaded to the user's laptop and/or further uploaded to a centralized web storage environment where the data would be accessible by additional information consumers.

Under a Low Battery condition, a user's role may change. For example, a family member, coworker, or complete stranger may be required to assist an individual with a pacemaker to contact medical facilities to recharge it. In doing so, these users' role changes to a nurse or administrator in which a patient's PII may be required to facilitate care. Additionally for other users, their role may not be assigned until the Low Battery condition applies. For example, a coworker or young family member may be required to recharge or change an instrument battery. At that point in time, their role is assigned and then they perform their duty.

#### 2.3.2.1.2 Lost Wireless Signal

With Bluetooth, Wi-Fi, and cellular wireless technologies, the distances between antennas, line-of-sight, and interferences may reduce data throughput or deny information flow entirely. Like the Low Battery condition discussed above, data availability may be hampered in part or entirely. For those instruments which utilize wireless technologies, a disrupted signal with reduced data throughput may dictate what information is transmitted. For example, a pacemaker with a poor Bluetooth signal may be detectable by the instrument which may then transmit only critical configuration information.

Also, a disrupted wireless hearing aid signal may require an assistant to plug the instruments into a computer via special wired connectors, thus completely bypassing the wireless line of communication. In this example, the data transmitted may increase or decrease because it is acquired by a user through the wired interface and because the wireless interface failed. For example, the wireless configuration settings, service set identifier (SSID), and security passphrase would not normally be transmitted via the wired interface, but, because the wireless interface is disrupted, this data may now be transmitted.

However, user role assignments may also change given a failed wireless connection. For example, a hearing aid user may request that a Local Area Network (LAN) administrator examine and repair the instrument's Bluetooth connection. The role of the LAN administrator then changes to a certified hearing aid professional. Another example involves the Zephyr Heart Rate monitor which also uses Bluetooth technology coupled with a smartphone. In this example, the user asks the local Verizon cell phone technician to diagnose a Bluetooth technical failure. Again the role of the cell phone technician changes to a Zephyr device technician. A fair amount of PII resides on the smartphone for the Zephyr Heart Rate monitor application and therefore the model should anticipate changes to user role assignments.



A network hardware failure (or lack of service) would negate transfer of health information. While a failed upload to Facebook or Twitter may only provide a slight annoyance, a failed upload to a hospital medical service may impair medical diagnosis in an urgent or even critical situation. Access to the same information may require user owner permission in the form of a password. A patient in distress may not be able to provide such authorization in order for emergency personnel to safely administer first-aid.

#### 2.3.2.1.3 Broken Connector

A broken wire connection will most likely disrupt a communication flow. A connection to an outside environment (e.g., usb connector, RS232 pin, firewire socket) would constitute a communications disruption similar to the lost wireless signal discussed above. However, an internally broken connection may cause other data availability impacts. For example, a broken connector pin between a hearing aid base and the receiver unit renders the instrument useless for the user. In this situation the data in the instrument remains intact and otherwise operates as designed. However, the hearing aid may not make all data available since the device should be returned to the manufacturer for repair. Any PII may become unnecessarily available to the repair operator. If the desire is to not make information contained within the instrument accessible to a repair operator, then the instrument could fail into a closed state, thus rendering the data unavailable.

In some situations, one would anticipate failing an instrument into a state wherein no data or perhaps only configuration data is made accessible to a repair operator via an operational interface. One could potentially configure an instrument to only provide such information under all failed and normal (e.g., check-up) conditions. However, some or all PII may be required to actually perform a diagnosis and to validate the instrument upon repair. From a modeling perspective, the roles for the user and repair operator do not change, just the access to whatever information is provided to the role upon an instrument failure.

Like the lost wireless signal, a user may consign an instrument administrator the role of a system technician in order to repair a broken connector. For example, the ICE Medical ID Card in Appendix A may suffer a corroded USB connection after the wallet, which protected it, fell into a water source. The user may ask the local pharmacist from the store the instrument was purchased to perform a repair. Given that the pharmacist is a kind individual, the role changes to hardware technician.

#### 2.3.2.1.4 Clogged Tube

Insulin pumps and hearing aids contain tubes which may at some time get congested or completely clogged. This situation is similar in nature to an internally broken connector described earlier. The potential impacts to data availability and user role assignments may change. For example, should an insulin pump suffer a clogged tube, then the medication cannot be accurately dispensed. The insulin pump may fail into a state wherein only the medication type and the dosage are displayed. All other information may be hidden and the instrument ceases all other functions. While this may cause a serious safety problem for the patient, it also translates into a situation where additional users may be authorized to access the limited amount of data and some users may be assigned new roles in order to repair the condition. Thus, this example of a safety issue is also an example of an information security issue.

#### 2.3.2.1.5 Low Medicine/Solutions

Insulin pumps include prescribed medications (insulin). Low or empty reservoir condition is similar in nature to a low battery condition described earlier. The potential impacts to data availability and user role assignments are similar to those of the clogged tube discussed above.

### 2.3.3 User Failure

This section highlights user failures that dynamically impact data availability and user role assignments. In Section 1, a new access control model is presented that can represent these failures and their changes to data access control protections.

Users of instrument “fail” in a variety of fashion. For example, a patient with a pacemaker is subject to heart conditions including [28] Bradyarrhythmias (slow heart rhythms), Hypertrophic Cardiomyopathy (thickening of the heart muscle), heart failure, or Syncope (fainting spells).

The Medical community has developed and adopted a set of codified medical conditions of patients into a hierarchical structure. Specifically, the “International Classification of Diseases (ICD) is designed to promote international comparability in the collection, processing, classification, and presentation of mortality statistics.”[29] While “mortality statistics” provide a “fundamental source of demographic, geographic, and cause-of-death information” [30], the ICD10-CM provides a means to help track diagnoses, manage patient care, and track injuries in the US medical community.

A few examples of these ICD10-CM codes [31] provide a useful reference for this thesis. These examples help demonstrate their contribution to the IS-RBAC model in Section 3.2.

S46.021 Laceration of muscle(s) and tendon(s) of the rotator cuff of right shoulder

S62.7 Multiple fractures of fingers

S62.511 Displaced fracture of proximal phalanx of right thumb

R40.222 Coma scale, best verbal response, incomprehensible words

R45.4 Irritability and anger

R45.5 Hostility

R45.6 Violent behavior

R45.7 State of emotional shock and stress, unspecified

S06.0x8 Concussion with loss of consciousness of any duration with death due to other cause prior to regaining consciousness

### 2.3.3.1 User Failure Impacts

Like instrument failures, user failures impact data availability and user role assignments in the instruments presented in this thesis. Several types of user failures are presented in Appendix B. Their ICD10-CM codes are included in this section. Table 2 summarizes these impacts. Further below, each of the three types of user failures is presented and the actual or possible changes in data availability and user role assignments are discussed.

Table 2. User failures and their impacts to user role assignments and data availability.

	Mental States; ICD10-CM Series R40 and R45	Arm/Hand Muscle Lacerations and Fractures; ICD10-CM Series S46 and S62	Death; ICD10- CM Series S06
Pacemaker	UA	-	UA
Insulin Pump	UA	UA	UA
Hearing Aids	UA	-	UA
H'andy Sana 210	UA, D	D	UA
Instant Heart Rate	UA, D	D	UA
Zephyr Heart Rate	UA, D	D	UA
ICE: In Case of Emergency	UA	-	UA
ICE Medical ID Card	UA	-	UA
Cardio Trainer	UA, D	D	UA
Electric Sheep	UA, D	D	UA
Ultrasound	UA	-	UA

UA = User Role Assignment impact

D = Data Availability impact

<dash> = Not Applicable

#### 2.3.3.1.1 Mental States

The mental state of a user impacts data availability of a Socio-Technical System. If the user provides a password for access to data or plays an integral part in data transfer or elicitation, then a failure of the user may result in a failure of these functions and limit the data that may be accessible. A few sample user mental states include “coma where their best verbal responses are incomprehensible words” (ICD10-CM R40.222 in Appendix B), irritable/angry, hostile, violent, shock, and stress ((ICD10-CM series R45.x in Appendix B).

Given such user mental states, data availability in an instrument may be affected. For example, if the user is in a coma, it would be rather difficult to self-operate the Instant Heart Rate application which relies on the user’s ability to place a finger over an LED on the smartphone instrument. Likewise, the H’andy Sana 210 application requires the user to place two fingers on separate contacts to complete an electric circuit.

Given such user mental states, user role assignments in a Socio-Technical System may also be affected. For example, an angry, stressed, or in-shock user may result in the addition of participating users such as a Good Samaritan to act in the role of a first responder (e.g., emergency medical technician (EMT)). In the case of an insulin pump, the good Samaritan may communicate with medical staff in order to increase or decrease insulin dosage.

As the scope of a Socio-Technical System expands to include administrators, operators, technicians, medical staff, etc., their mental states also affect other user role assignments. Basically, the mental state of these additional users may render their participation as ineffective as if the instrument owner’s own mental state were impaired. If a medical staff participates in information flow and they are the one mentally incapacitated, then user role assignments may change. For example, an ambulance driver may take on the role of an EMT if the EMT’s mental state is compromised (e.g., ambulance traffic accident).

Finally, the user's mental state may reach a point of long term incapacity. In such a circumstance, legal responsibility of the user care and data ownership comes to bare. The discussion regarding death covers the impact this may have on user role assignments, specifically data ownership.

#### 2.3.3.1.2 Lacerations and Fractures

Like the mental states discussed above, lacerations and fractures of the arm/hand of a user may render their participation ineffective in a Socio-Technical System. This physical limitation follows the same incapacity as the limitations of users' mental states discussed above. The impacts to data availability and user role assignments follow the same results. However, with physical limitations, a user may still be able to participate in the Socio-Technical System by providing information to other participants verbally.

#### 2.3.3.1.3 Death

ICD10-CM Series S06 involves death of the user. Dimick [32] questions the complicated legal questions associated with confidentiality of PII when a data owner dies (the ultimate user failure). He writes,

A son calls the HIM department and requests his deceased father's medical records. Shortly afterward, the man's wife requests the records, also. Then a man calls identifying himself as the executor of the estate. Who is authorized to access the records?

Determining appropriate release of a deceased patient's medical records can be complex. HIPAA, sometimes blamed for denied requests, is rarely cause for a roadblock, however. The federal law does extend a person's privacy rights into death, but it also explicitly requires facilities to release records to authorized individuals.

While this thesis does not discuss legalities of data ownership, the fact that a user failure (especially the ultimate failure) changes expected and legal authorized access to information remains an imperative point. By definition, the death of the user impacts the Socio-Technical System. Elimination of the (only) participatory user from a Socio-Technical System may

transform it to just a Technical-computer system. Access assignments for the remaining users of a Socio-Technical System should be explicitly defined or implicitly understood a priori to a user owner death in order to eliminate unauthorized information disclosures.

While the death of a user is not a pleasant topic, it does present serious ramifications to user role assignments. Specifically, the legal owner of the information stored in the Socio-Technical System changes, even if the new owner is the original user's legal estate. For the original user of the Socio-Technical System, the concept of data availability issues becomes irrelevant, except for perhaps the new data owner. If the original user was irrevocably involved with the protection of data stored within the instrument or other component of the Socio-Technical System, then perhaps data availability for the new data owner becomes relevant. For example, if the original user maintained a password/phrase that granted root-like access to the data, then the new owner may require other technical solutions to acquire the data. A forensic analysis may be required under these conditions which also introduce actors who will gain full access to data stored within the instrument.

## **2.4 Environmental Situations**

This section highlights instrument failures that dynamically impact user role assignments. In Section 1, a new access control model is presented that can represent these failures and their changes to data access control protections.

Some environmental situations control the roles users are assigned. Some users may be required to perform duties with elevated privileges normally reserved for other users. In such a case, some user role assignments may change.

When a user's role assignments change with the given conditions of the environment, the user should not necessarily retain all access assignments for each environmental situation at the

same time. The problem with combining all of a user's access assignments is that users may acquire different levels, types, complementary, or contradictory accesses.

Table 3 summarizes three environmental situations that influence data availability and user role assignments for the Socio-Technical Systems presented earlier. Each situation is discussed further below.

Table 3. Environmental situations and their impacts to user role assignments and data availability.

	Hospital Code Red	Airplane mode	Displaced
Pacemaker	UA	UA, D	UA, D
Insulin Pump	UA	UA, D	UA, D
Hearing Aids	UA	UA, D	UA, D
H'andy Sana 210	UA	UA, D	UA, D
Instant Heart Rate	UA	D	UA
Zephyr Heart Rate	UA	UA, D	UA
ICE: In Case of Emergency	UA	D	UA
ICE Medical ID Card	-	-	UA
Cardio Trainer	-	D	UA
Electric Sheep	-	D	UA, D
Ultrasound	UA	-	UA

UA = User Role Assignment impact

D = Data Availability impact

<dash> = Not Applicable



### **2.4.1 Hospital Code Red**

During normal hospital situations, Registered Nurses (RNs) would only have authorized access to a portion of patient information and only to those patients assigned to their ward. A patient who becomes violent, a missing child in the hospital, a (localized) fire, may trigger a “Code”. In a “code red” situation, the Hospital administrators may establish that all RNs may gain access to all patient data in order to potentially help with patient care outside their normal duty stations.

A large volume of patients may arrive at an emergency room in which a triage must be conducted. A major catastrophe may also befall a hospital such as an earthquake, large scale fire, or widespread area flooding. In such situations, a nurse may assume the role of a doctor, a clerk may assume the role of a trauma nurse, and a Good Samaritan may provide first responder care (determine patient vital signs).

Medical personnel are subject to the same disabling diseases as patients and thus a shortage of staff may arise. Medical personnel get called away and operational workloads may contribute to situations in which roles and responsibilities become greater for some personnel when otherwise would be reduced under normal conditions.

In each of these situations, each person’s explicit or implicit “authorized” access to information changes. It should be noted that the specific roles do not necessarily change (but they might); e.g., an RN in the nursery ward, third floor, south, remains the same. However, in a code situation, they may be called upon to perform specific functions normally reserved for users in different roles.

### **2.4.2 Airplane Mode**

A user’s smartphone is sometimes considered an integral part of a Socio-Technical System. Current FAA regulations prohibit transmission of cellular or Wi-Fi or Bluetooth

transmissions while airborne. This situation illustrates that there are environmental conditions that affect a Socio-Technical System and not just network or instrument failures. The result of placing a device in Airplane mode should reflect the same impacts on those Socio-Technical Systems as those instrument failures described in Section 2.3.2.

### **2.4.3 Displaced**

A displaced instrument arises when a user loses their smartphone, a broken hearing aid is returned for repair, or an obsolete pacemaker is replaced. Like the death of the user, by definition this displacement of the instrument impacts the Socio-Technical System. Elimination of the participatory user's instrument from a Socio-Technical System may transform it to just a user without a major Technical Computer-Based System component. A displaced instrument is identical to the death of a user, from the perspective of the instrument; e.g., a lost instrument becomes a Technical Computer-Based System without an authorized user. Someone who locates a displaced instrument may then conduct a forensic analysis and may gain full access to data stored within the instrument. Authorized access to the instrument and to the remaining components of a Socio-Technical System should be explicitly defined or implicitly understood when an instrument becomes displaced. This will help eliminate unauthorized information disclosures of PII.

## **2.5 Data Availability and User role assignments**

This section reviews the content of the previous sections with respect to data availability and user role assignments. This will guide the structure of the IS-RBAC model presented later in Section 3.1.

Sommerville [5] defines Socio-Technical Systems as Technical Computer-Based Systems with

defined operational processes,  
include people (operators [users]) as inherent parts of the system  
are governed by organizational policies and rules  
affected by external constraints such as national laws and regulatory policies.

Socio-Technical Systems characterize instruments, computer systems, and users discussed previously. The instrument failures arise within and at the boundaries of the Technical Computer-Based Systems. The user failures arise also within and at the boundaries, given that people are inherent parts of the Socio-Technical System. Finally, the environmental situations directly impact the operational processes of a Socio-Technical System.

The impact of instrument failures, user failures, and environmental situations to Socio-Technical Systems appears in two areas. The first area affects the availability of data. For example, a broken network interface would prevent data transfer and thus deny data availability through that interface. However, another aspect of data availability lies with user interactions. For example, in order to transfer information from one entity to another, a system procedure may require a user to enter a password. The classic interpretation of availability disregards such user interactions and draws the distinction that the system availability boundary ends with the ability to allow the user to enter the password and not include the user's interactions as part of the system. While true for a Technical Computer-Based System, one could expand the system availability boundary to include user interactions as part of a Socio-Technical System. For the purpose of this model, we will attempt to represent the impact of user interactions on the availability of data within Socio-Technical Systems.

The second area affects the user role assignments. Thus the model should represent data conditional confidentiality. Given that Technical Computer-Based Systems may include multiple

data interfaces, failure of one data flow interface (or other instrument) does not necessarily negate data flows through the other data interfaces (or other instruments). However, when such failures occur, the access assignments to the data may change. Our model must reflect this quality of Socio-Technical Systems.

### **2.5.1 Data Availability**

Instrument failures affect a Technical Computer-Based System directly. When a device fails, its operational state changes. In failed states, the instrument may not be able to provide data to the user. By definition, availability is the ability to provide data. Therefore, an instrument's operational state affects the availability of instrument provided data.

User failures affect Socio-Technical Systems in the same fashion as instrument failures. When a user "fails", her participation in the Socio-Technical System becomes inhibited. For example, she may not be able to provide a password or consent physically and/or mentally. As such, the devices which store information may not be able to be accessed under normal conditions. Therefore, a user's operational state can directly affect the availability of instrument provided data.

### **2.5.2 User Role Assignments**

Instrument failures also affect Socio-Technical Systems. When a device fails, its operational state changes. In failed states, the instrument may still be able to provide data via other interfaces.

User failed states may affect access assignments of other personnel through existing and working instrument interfaces. Changes to data access assignments may be explicitly taken into account in anticipation of a user failure, since one may need to rely on another to enter such data or act on their behalf. Thus, a user's failed states affect user data access assignments.

Like instrument and user failures, environmental situations affect Socio-Technical Systems. User role assignments change given emergency situations and availability of other participants in the Socio-Technical System.

We need a model that can establish user role assignments based on three new influences. Fortunately, the RBAC model provides a starting point.

## 2.6 RBAC

This section reviews several access control models. This background information provides a starting point for development of the IS-RBAC model in the next section.

### 2.6.1 Basic RBAC

Sandhu, et al. [33] present the RBAC model. It establishes users, roles, and the role permissions within the confines of a single session. Sandhu, et al. [33] define RBAC with the following components:

$U, R, P$ , and  $S$  (users, roles, permissions and sessions respectively),

$PA \subseteq P \times R$ , a many-to-many permission to role assignment relation,

$UA \subseteq U \times R$ , a many-to-many user to role assignment relation,

$user : S \rightarrow U$ , a function mapping each session  $s_i$  to the single user  $user(s_i)$  (constant for the session's lifetime),

$roles : S \rightarrow 2^R$ , a function mapping each session  $s_i$  to a set of roles  $roles(s_i) \subseteq \{r \mid (user(s_i), r) \in UA\}$  (which can change with time) and session  $s_i$  has the *permissions*  $\cup r \in roles(s_i) \{p \mid (p, r) \in PA\}$ . We expect each role to be assigned at least one permission and each user to be assigned to at least one role. The model, however, does not require this.

### 2.6.2 Context Sensitive

Hulsebosch [34], et al. present the concept of a “Context sensitive access control” model. A user’s geographic location, device capabilities (battery power, memory, operating system), Network type (wifi, GSM) plays a part in determining user role assignments/rights. The

conclusion of their research resulted in “a relatively strong, less intrusive and more flexible access control process that mimics our natural way of authentication and authorization in the physical world.” The “device capabilities” could potentially represent instruments in a Socio-Technical System. However, the model discussed by Hulsebosch does not include references to RBAC or any formal specification of an access control model.

### **2.6.3 GeoTemporal**

Atluri [35], et al., present the concept of a “Geotemporal role-based authorization system.” In this model, the researchers extend the RBAC model as a “geotemporal role pair  $\langle r, sc \rangle$  where  $r$  is a traditional role for subjects as in RBAC role hierarchy, and  $sc$  is a scene that can be associated with a set of geospatial and temporal extents.” Formalisms for geospatial bounded boxes, and associated logical and functional operators are presented. This allowed the researchers to “specify subjects like ‘all the policemen who are in the fire scene’ or ‘all the shoppers in the mall during Christmas season’.” Based on these extensions, the RBAC model was able to represent a finer granularity of information access to users.

In a similar fashion, Ray and Toahchoodee [36] present a “Spatio-Temporal” RBAC model. The location and time are represented and relate to users as atomic expressions. These expressions provided a means to “activate” and “restrict” locations and temporal elements and were combined with user role assignments and with “session roles”, respectively.

### **2.6.4 Fuzzy RBAC**

Nawarathna and Kodithuwakku [37] introduce the Fuzzy RBAC model. FRBAC “adds a new component called policy administration which models the organization security policies using a fuzzy approach.” Essentially, the policies associated with permission assignments PA are effectively not so readily assigned. The PA computation is conducted in a dynamic fashion and

utilizes a “fuzzy policy evaluator (FPE)”. With the FPE a dynamic permission assignment (DPA) is computed based on fuzzy data sensitivities and rules.

### 2.6.5 Privacy Sensitive RBAC

Q. Ni, et al.[38] summarizes Privacy Sensitivity RBAC (P-RBAC) as follows

In P-RBAC, privacy policies are expressed as permission assignments (PA); these permissions differ from permissions in classical RBAC because of the presence of additional components, representing privacy-related information. The resulting model is clean and leverages the success of RBAC. However, because in our approach PRBAC policies may be authored by different users and also they may include a large variety of conditions, conflicts among PA may arise. To address such issue, in the paper we also develop conflict analysis algorithms to detect conflicts among PA, thus avoiding the problems that Enterprise privacy authorization language (EPAL) [IBM Zurich Research Laboratory, Switzerland ] rules have because of its sequential semantics Barth et al.[39].

Due to the complexity and variety of privacy policies and privacy requirements from different organizations, we employ a “Divide and Conquer” methodology. That is, the models in our P-RBAC family are designed to meet different levels of requirements and handle different problems. The P-RBAC family includes four models: Core PRBAC, Hierarchical P-RBAC, Conditional P-RBAC and Universal P-RBAC. Core P-RBAC is the basic model and is able to directly represent privacy-crucial information, such as purpose of data use and obligations. However, although Core P-RBAC can be used to describe commonly used public privacy policies and some acts, the limited expressiveness of its condition language makes it not suitable for representing internally enforceable privacy policies for large scale enterprises and/or complex applications. Specifically, Core P-RBAC has the following limitations. First, Core P-RBAC only supports equality constraints on context variables in finite domains. Second, conditions are restricted to conjunctions of atomic formulas. Third, it only supports one type of relation, that we refer to as AND, among different permission assignments. The type of relation adopted by a set of permission assignments is crucial in determining which obligations need to be executed and which conditions have to be meet[ing] when several permissions may apply to the same request.

A major shortcoming of Core P-RBAC is the limited expressive power of its condition language LC0. For example, LC0 is not able to express conditions like (DataUser=“Alice”) OR (DataUser=“Bob”) because it only supports conjunction as logical operator. LC0 cannot deal with conditions like (8am < currentTime < 5pm) either because it only supports equality comparisons. However, enhancing the expressiveness may result in a condition language which is not tractable. In particular, to determine whether a condition in a permission assignment can be satisfied is essentially the classic NP-complete satisfiability problem (SAT) where only a few classes of formulae are

tractable. Therefore, for practical purposes, we divide our problem into two subcases, a tractable case and an intractable case, by carefully investigating commonly used conditions in privacy policies. Correspondingly, we define Conditional P-RBAC as characterized by a two-fold solution as follows.

- We define a more expressive condition language LC1 and introduce the concept of simple permission assignment set, for which SAT is tractable.
- We define a fully expressive condition language LC2 and introduce the concept of advanced permission assignment set, for which SAT is theoretically intractable but remains tractable in practice given a reasonable assumption.

The “conditional P-RBAC” by Q. Ni et al. [38] at first glance looked like it might potentially represent the mechanical failings, user failings, and environmental situations discussed in this thesis. However, the “conditional” portion of Q. Ni’s [38] model added numerous logical operators above the standard conjunction (“AND”) operators found in Core-P-RBAC. With disjunction operators, intractable situations arise. Q. Ni, et al, [38] provides an algorithmic solution to intractable forms. “Conditional P-RBAC supports more expressive condition languages and more flexible relations between permission assignments.”

The “hierarchical P-RBAC” by Q. Ni et al. [38], “provides role hierarchies, data hierarchies, and purpose hierarchies.” The role hierarchy is used to represent organization structures, lines of authority, and areas of responsibilities. Data hierarchies presume that access to a parent node data element is allowed only when access to all of its children node data elements is granted. Finally, purpose hierarchy allows structure to relate information purposes. Like the data hierarchy, access to a parent node purpose is only granted when access to all of its children nodes are granted.

The “universal P-RBAC” portion of the model “combines Hierarchical P-RBAC and Conditional P-RBAC, and inherits both their features. Such integration of Hierarchical P-RBAC and Conditional P-RBAC supports the specification of more complex relations between different permission assignments.” A universal data model might be considered ambitious, yet it may in



fact provide a solution to help represent instrument failures, user failures, and environmental situations.

### **2.6.6 Adding Attributes**

Kuhn, et al. [40] discuss a perspective on how attributes can be added to RBAC model. Attribute-based access control (ABAC) “might be more flexible than RBAC [because] it does not require separate roles for relevant sets of subject attributes, and rules can be implemented quickly to accommodate changing needs.” However, the complexity of an ABAC lies in its complexity of combining attributes. Kuhn combines RBAC and ABAC as a strategy. The strategy employs the combination of users, roles, and/or attributes. For example, by using just users and roles, one achieves the basic RBAC model. Likewise, by using just attributes, one achieves the basic ABAC model. In total, ten combinations can be derived. The last three strategies use all three elements, but in different quantities. Roles with attributable names constitute a attribute-centric approach. Attributes that constrain roles constitute a role-centric approach. Finally, the use of “dynamic” roles, results in a dynamic role approach.

### **3 Impediment Sensitive - RBAC Model**

This thesis presents a variation of the RBAC model. It is termed an Impediment Sensitive RBAC (IS-RBAC) model and may be applied in a Socio-Technical System. This section presents a short review of the models discussed so far, the requirements per se of the IS-RBAC model, and the source of the “Impediments”. This short review describes the new functionality and goals of IS-RBAC. Subsequently, the definition of IS-RBAC and an example are presented.

The complex P-RBAC model is not necessary to represent all the Socio-Technical Systems presented in this thesis. For example, the ICE Medical Card and the “Electric Sheep” application in Appendix A only involve a few actors and potential Technical Computer-Based Systems. However, for some of the Socio-Technical Systems discussed, a model that is based on a robust P-RBAC would be useful. For example, the Zephyr Heart Rate Monitor and the Insulin Pump applications involve several actors and Technical Computer-Based Systems and potentially a variety of data consumers across the Internet. However, a complex RBAC model such as P-RBAC does not address the impediments, their implications to user role assignments, or the availability of data.

Some RBAC models and variations integrate users, but without consideration of their function as within a Socio-Technical System. User role assignments, attributed to a user, correctly assume that the user is the ultimate direct consumer of data and outside the boundary of a Technical Computer-Based System, e.g., not an integral part of the system. With a Socio-Technical System, data not only directly flows to and from a user, but data also potentially flows through a user to another user or Technical Computer-Based Systems, all of which make up the total Socio-Technical System.

The complex models that Q. Ni [2] employ treat users on the fringe of a Technical Computer-Based System; the Hierarchical P-RBAC, Conditional P-RBAC and Universal P-RBAC. Q. Ni [2] provides a “more expressive condition Language(s)” LC1 and LC2 which introduces the concept of “simple permission assignment set” and “advanced permission assignment set”, respectively. The LC0 includes conjunction logical operator and equality comparisons. The LC1 provides additional conditional operators such as or, less than, greater than. However, they do not address aspects of data and instrument availability nor environmental situations.

The issue is that all of the RBAC models can be used to represent a user, but none represent user failures (or user failure states). Similarly, instruments could potentially be represented by ordered, unordered, hierarchical, or any of a dozen “list” representation sets. But equally, none represent instrument failures (or instrument failure states).

Likewise, the model needs dimensions in order to represent instrument failures, user failures and environmental situations. The model should also represent of user role assignments and ultimately access controls to information. Finally, the model needs to represent impacts to data availability.

The combination of instrument failures, user failures, and environmental situations reflect the “impediments” as described in Section 2.3.1. User medical conditions which prohibit or otherwise impair a user’s ability to participate in authentication effectively degrades the integrity of authentication and therefore breaks the mechanism by which confidentiality is enforced. The immediate consequence of these impediments results in marginal to full data availability constraints. However, ultimately, these impediments result in changes to user role assignments which in turn result in changes to access controls which goes to data confidentiality. In the

following sections we introduce an RBAC model sensitive to impediment failures and situations call IS-RBAC.

### 3.1 IS -RBAC Definitions

In this section, we introduce the IS-RBAC model with 5 new definitions. As each definition is presented, the model solidifies a representation of how instrument failures, user failures, and environmental situations impact both data availability and user role assignments. Ultimately, the change in the data set and the set of user role assignments affect the access control model at its foundation.

Definition 1. From Sandhu, et al.[33], we take the following components:

- $U, R, P,$  and  $S$  (users, roles, permissions and sessions respectively),

Definition 2. The IS-RBAC model must represent data, a conditional language, instrument failures (or instrument availability states), and user failures (or user availability states). In addition to Definition 1 above, we begin the development of the new model with the following components:

- A set  $D$  of data
- A conditional language  $LC$
- A set  $I$  of instruments, a set  $S$  of operational states, a set  $E$  of environmental situations.
- How does an instrument operational state dictate availability of data? An instrument's operational state affects the instrument's ability to provide data. By definition, availability is the ability to provide data. Therefore, an instrument's operational state affects the availability of instrument provided data.
- $M = \text{Instrument Availability States} \subseteq I \times S$ , a many-to-many instrument to operational state assignment relation.

- How does a user operational state dictate availability of data? A user's operational state affects the user's ability to provide data or ability to authorize use of data. By definition, availability is the ability to provide data. Therefore, a user's operational state affects the availability of user provided data.
- $Y = \text{User Availability States} \subseteq U \times S$ , a many-to-many user to operational state assignment relation.
- How do the environmental situations dictate availability of data? While Environmental situations may affect the ability of an instrument or user to operate (i.e., Electro Magnetic Pulse), the result of such a situation should be covered by the instrument and user availability states presented above. However, environmental situations may affect the instrument's and/or user's expectations to provide and/or consume data. For example, building lockdown, martial law, and medical "code red" effect which users are assigned specific roles. Therefore, environmental situations affect user assignments.
- $Z = \text{User Availability States} \subseteq U \times E$ , a many-to-many user to environmental situation assignment relation.

Definition 3. The IS-RBAC model must represent changes to data availability based on the instrument availability states  $M$  and user availability states  $Y$  shown in Definition 2. The new data sets  $D'$  and  $D''$  shown are derived from the original data set  $D$ , shown in Definition 1, and are sensitive to these  $M$  and  $Y$  availability states, respectively. These two new data sets are then combined into a data set  $D'''$ . In order to assure no duplicate data elements in  $D'''$ , we take the union of  $D'$  and  $D''$ .

- The set of Instrument Impediment Sensitive Data
  - o  $D' = \{(d, \mu) \mid d \in D, \mu \in M\}$
- The set of User Impediment Sensitive Data
  - o  $D'' = \{(d, v) \mid d \in D, v \in Y\}$

- The set of all Impediment Sensitive Data

- o  $D''' \subseteq \{D' \cup D''\}$

Definition 4. We can now utilize the new set the Impediment Sensitive Data  $D'''$  from Definition 3 and the set of users  $U$ , instruments  $I$ , and the conditional language  $LC$  from Definition 2 in order to define impediment sensitive data permissions  $IPD$  and their respective role assignments ( $IDPA$ ). The  $IDPA$  definition will be used in lieu of the permission to role assignment  $PA$  from the original RBAC model, which does not take into account data or data sensitivities to impediments.

- The set of Impediment-sensitive Data Permission  $IDP = \{(u, i, d, p, c) \mid u \in U, i \in I, d \in D''', p \in P, c \text{ is an expression of } LC\}$
- The set of Impediment-sensitive Data permission Assignment  $IDPA \subseteq R \times IDP$ , a many-to-many impediment-sensitive data permission to role assignment relation.

Definition 5. Instrument and user availability states also affect user role assignments. We represent this by preparing a many-to-many mapping of instrument and user availability states from Definition 2 to the user role assignments  $UA$  in RBAC. Likewise, Environmental Situations affect user role assignments. The result of the instrument and user availability states yield a final set of user role assignments as follows:

- The set of User Availability Sensitive User role assignment
  - o  $UA' \subseteq Y \times R$ , a many-to-many user availability states to role assignment relation.
  - o This is identical to the User role assignment in RBAC except that the set of users  $U$  has been replaced with the set of User Availability States  $Y$  shown in Definition 2.

- The user's availability controls the roles users are assigned, such as when the user is non-responsive and cannot provide the password to retrieve data from the instrument. In such a case, some user assignments to certain roles may change.
- The set of Instrument Availability Sensitive User role assignment
  - $UA'' \subseteq M \times R$ , a many-to-many instrument availability state to role assignment relation.
  - This is identical to the User role assignment in RBAC except that the set of users  $U$  has been replaced with the set of Instrument Availability States  $M$  shown in Definition 2.
  - The instrument's availability controls the roles users are assigned, such as when the medical device is in low power and cannot connect to a wifi network to transmit data. In such a case, some user assignments to certain roles may change.
- Finally, Environmental situations may control the roles users are assigned, such as when the environmental situation in a hospital emergency room changes to a (medical) code red. Some users (nurses) may be required to perform duties with elevated privileges normally reserved for other users (doctors). Thus, we formulate a second set of User Availability Sensitive User role assignment.
  - $UA''' \subseteq Z \times R$ , a many-to-many user availability state (due to environmental situations) to role assignment relation.
  - Like the definition for  $UA'$ , the definition of  $UA'''$  is identical to the User role assignment in RBAC except that the set of users has been replaced with the set of User Availability States  $Z$  which are sensitive to environmental situations as shown in Definition 2.
  - The environmental situations control the roles users are assigned, such as when a hospital is placed under a code red situation and then nurses may act as a

physician's assistant. In such a case, some user assignments to certain roles may change.

- The User role assignments  $UA'$ ,  $UA''$ , and  $UA'''$  need to be combined. A simple union accomplishes this task.
  - o  $UA'''' \subseteq \{UA' \cup UA'' \cup UA'''\}$ , an impediment sensitive user role assignment relation.

Definition 6. The impediment-sensitive data permission assignments  $IDPA$  of Definition 4 effectively replace the permission role assignment  $PA$  in RBAC. However, the definition of the user session relies upon  $PA$ . Additionally, the impediment sensitive user role assignment  $UA''''$  from Definition 5 replaces the user role assignment  $UA$  in RBAC. Therefore, a slightly new definition of a session is required. The changes to the session definition are shown below in bold underline.

$user : S \rightarrow U$ , a function mapping each session  $s_i$  to the single user  $user(s_i)$  (constant for the session's lifetime), and

$roles : S \rightarrow 2^R$ , a function mapping each session  $s_i$  to a set of roles  $roles(s_i) \subseteq \{r \mid (user(s_i), r) \in \underline{UA''''}\}$  (which can change with time) and session  $s_i$  has the (**impediment sensitive data**) permissions  $\cup r \in roles(s_i) \{ \underline{idp} \mid (\underline{idp}, r) \in \underline{IDPA} \}$ .

The final collection of IS-RBAC definitions include the following:

- $U, R, P, D$ , and  $S$  (users, roles, permissions, data, and sessions respectively),
- A conditional language  $LC$
- $I, S, E$  (instruments, operational states, and environmental situations, respectively),
- $M = \text{Instrument Availability States} \subseteq I \times S$ , a many-to-many instrument to operational state assignment relation.
- $Y = \text{User Availability States} \subseteq U \times S$ , a many-to-many user to operational state assignment relation.



- $Z = \text{User Availability States} \subseteq U \times E$ , a many-to-many user to environmental situation assignment relation.
- $D' = \{(d, \mu) \mid d \in D, \mu \in M\}$ , The set of Instrument Impediment Sensitive Data
- $D'' = \{(d, v) \mid d \in D, v \in Y\}$ , The set of User Impediment Sensitive Data
- $D''' \subseteq \{D' \cup D''\}$ , The set of all Impediment Sensitive Data
- $IDP = \{(u, i, d, p, c) \mid u \in U, i \in I, d \in D''', p \in P, c \text{ is an expression of LC}\}$ , The set of Impediment-sensitive Data Permissions
- $IDPA \subseteq R \times IDP$ , Impediment-sensitive Data permission Assignment, a many-to-many impediment-sensitive data permission to role assignment relation.
- $UA' \subseteq Y \times R$ , a many-to-many user availability states to role assignment relation.
- $UA'' \subseteq M \times R$ , a many-to-many instrument availability state to role assignment relation.
- $UA''' \subseteq Z \times R$ , a many-to-many user availability state (due to environmental situations) to role assignment relation.
- $UA'''' \subseteq \{UA' \cup UA'' \cup UA'''\}$
- $user : S \rightarrow U$ , a function mapping each session  $s_i$  to the single user  $user(s_i)$  (constant for the session's lifetime), and
- $roles : S \rightarrow 2^R$ , a function mapping each session  $s_i$  to a set of roles  $roles(s_i) \subseteq \{r \mid (user(s_i), r) \in UA''''\}$  (which can change with time) and session  $s_i$  has the (impediment sensitive data) permissions  $\cup r \in roles(s_i) \{idp \mid (idp, r) \in IDPA\}$ .

### 3.2 IS-RBAC Example

The example in this section will draw upon the insulin pump described in Section 2.2.1. A description is provided of the Socio-Technical System and its two Technical Computer-Based Systems. Also described are their operational conditions, four different failures, users, and the types of accesses to the patient's PII. A discussion of the accesses is also provided. Finally, this same information is presented using the IS-RBAC definitions.

### **3.2.1 IS-RBAC Example Description**

The device chosen for this example is the insulin pump described in Section 2.2.1. Let's allow the device to be configured and modeled without IS-RBAC and then with IS-RBAC. The application of IS-RBAC will illustrate how it helps mitigate threat actors towards a patient's PII.

We introduce four impediments. The first and second impediments are system failures, specifically a clogged tube in the insulin pump and an overload on the Web Server. The third impediment is a user failure, specifically, the patient will suffer a type of coma. The fourth impediment is an environmental situation, specifically a Hospital Code Red situation.

The patient information stored in the device which requires protection includes the following: name, patient identity number, home address, birth date, type of diabetes, and insulin dosage. A variety of roles are used including the patient, spouse, physician, physician assistant, etc. The permissions for the user roles include Create, Delete, Read, and Update (CDRU).

### **3.2.2 Unanticipated Role Accesses**

Prior to the application of IS-RBAC, expected user roles access controls may be defined. However, some unforeseen circumstances may occur such as instrument and user failures and environmental situations which without proper thought could allow elevated privileges. This section depicts such a situation for access to patient PII, located within a Socio-Technical System made up of two Technical Computer-Based Systems (TCBS). The first TCBS is an insulin pump worn by the patient, such as the one described in Section 2.2.1. The second TCBS is the Web server that hosts the PII, such as the Google Health or Google Analytics also described in Appendix A. This section describes four user-roles and their access types to the patient's PII on the two TCBS, respectively. The access is partitioned into four types: create (C), read (R), update (U), and delete (D). The types of failures are described earlier in Section 2.3.

The elevated privileges, as a result of failure, negatively impact the confidentiality, availability, and integrity of the Patient's PII. These impacts weaken the protections of the Patient's PII, expose the data to threat actors, and potentially harm the privacy or even safety of the Patient.

Table 4 shows the access controls to a patient's PII, located on the insulin pump, for the Patient and Hospital Nurse roles. The access controls here lack proper consideration of failures and environmental situations. We see that under normal conditions the Hospital Nurse has no access to the patient's PII. However, given any type of impediment situation, the Hospital Nurse gains full CDRU privileges.

One could argue that the elevated privileges are the result of good intentions to allow the Hospital Nurse to provide uninhibited medical care. However, the principle of least privilege begs the question as to whether the Hospital Nurse truly requires full access to the patient's PII under these conditions. The intentions of the Hospital Nurse may result in harm to the Patient. Specifically, the Hospital Nurse could affect the confidentiality of the Patient's PII in the insulin pump by disclosing it to unauthorized persons. Such an act would violate the Patient's privacy, especially given HIPPA regulations. The Hospital Nurse could affect the availability of the Patient's PII in the insulin pump by disabling its display either intentionally or accidentally. This could affect the safety of the Patient since other users, including the Patient, may be denied access to the dosage or medication data. The Hospital Nurse could affect the integrity of the information in the insulin pump by changing the dosage settings. Such a change could adversely affect the safety of the Patient.

Table 4. Expected and unforeseen access to patient PII located on the insulin pump.

Roles	Expected	Unforeseen		
	Normal Conditions	Insulin Pump Clogged Tube	Patient Failure: Coma scale, best verbal response, incomprehensible words (R40.222)	Environment: Hospital Code Red
Patient	CDRU	CDRU	CDRU	CDRU
Hospital Nurse		CDRU	CDRU	CDRU

Table 5 shows the access controls to a patient's PII located on the web server for the Patient, Physician's Assistant, Web Server Global Support, and Web Server Technical Support roles. Here too we see the access controls lack proper consideration given a Web Server Overload failure. We see that under normal conditions the web support roles have no access to the patient's PII. But, as soon as there is a Web Server Overload, users in both support roles gain full CDRU privileges.

One could argue that the elevated privileges are the result of good intentions to allow the support users to provide uninhibited repairs to the server should, in the unlikely event, a Patient's PII becomes the source of a system failure. However, the principle of least privilege begs the question as to whether these support roles truly requires full access to the patient's PII under these conditions. Their intentions may include a sinister goal which may result in harm to the Patient.

Specifically, the Web Server Technical Support user could affect the confidentiality of the Patient's PII on the Web Server by disclosing it to unauthorized persons across the Internet. Such an act would violate the Patient's privacy, especially given HIPPA regulations. The Web Server Global Support user could affect the availability of the Patient's PII on the web server by moving content to other locations in the web server's file structure either intentionally or accidentally (e.g., backup and delete original). This could affect the safety of the Patient since

other users, including the patient’s physician, may be denied access to the dosage or medication data at a point in time when the patient suffers from a serious condition (e.g., insulin shock). The support users could affect the integrity of the information on the web site by deleting the patient’s data. Such a change could also adversely affect the safety of the Patient.

Table 5. Expected and unforeseen access to patient PII, located on the web server.

Roles	Expected	Unforeseen		
	Normal Conditions	Web Server Overload	Patient Failure: Coma scale, best verbal response, incomprehensible words (R40.222)	Environment: Hospital Code Red
Patient	CDRU	CDRU	CDRU	CDRU
Physician Assistant	R		CDRU	CDRU
Web Server Global Support		CDRU		
Web Server Technical Support		CDRU		

### 3.2.3 Authorized Role Accesses

Table 6 and Table 7 depict the authorized IS-RBAC to patient PII, located within the Socio-Technical System presented in Section 3.2.2.

Table 6. Authorized IS-RBACs to patient PII located on the insulin pump.

Roles	Normal Conditions	Insulin Pump Clogged Tube	Patient Failure: Coma scale, best verbal response, incomprehensible words (R40.222)	Environment: Hospital Code Red
Patient	CDRU	R	CDRU	CDRU
Physician	CDRU	R	CDRU	CDRU
Physician's Assistant	CDRU	R	CDRU	CDRU
Employer			R	
Web Server Global Support				
Web Server Technical Support				
Hospital Nurse		R	RU	R
Hospital Technical Support				
Patient's Online Pharmacist				
Paramedic			R	
Ambulance Driver			R	

NOTE: the grayed cells will be used as a sample session.

Table 7. Authorized IS-RBACs to patient PII located on the Web Server.

Roles	Normal Conditions	Web Server Overload	Patient Failure: Coma scale, best verbal response, incomprehensible words (R40.222)	Environment: Hospital Code Red
Patient	CDRU	CDRU	CDRU	CDRU
Physician	R		R	R
Physician's Assistant	R		R	R
Employer			R	
Web Server Global Support		R	CDRU	
Web Server Technical Support		R		
Hospital Nurse			R	R
Hospital Technical Support			R	R
Patient's Online Pharmacist	R		R	R
Paramedic			R	
Ambulance Driver				

NOTE: the grayed cells will be used as a sample session.

A discussion of the accesses for each type of user role is in order. The patient has the same accesses to the PII located in both the insulin pump and web server regardless of the type of failure, even when the patient fails into a coma, yet cannot express a password to retrieve the information. In this case, the patient doesn't have access to much of anything anyway. The only information available on the insulin pump may be displayed without the use of a password or, more importantly, if the insulin pump has a clogged tube, is the medication and dosage. It is

assumed that users who are authorized to CDRU other data fields will retain and protect a (pin number) password. This user failure in the role of the patient will play an important part in the user role assignment discussed further below.

The physician and physician's assistant have identical accesses. Full access is provided to the PII located in the insulin pump but only reader access to the PII located on the web server. This is because the insulin pump is the primary source of PII and thus is the location from which these users provide their service. The web server is a source by which they only read the information.

The employer, paramedic, and ambulance driver will all participate as good Samaritans and will be able to read the patient's PII located on the insulin pump. However, because the employer has an explicit relationship with the patient (employee) and because the paramedic (but not the ambulance driver) has an implicit relationship with the patient, they will be able to read the patient's PII from the web site if the patient suffers from a coma (or other incapacitating failure).

The web server technical (and global) support users gain access to the patient's PII online, should the web server suffer a failure. The web server global support users gain full CDRU access, should the user suffer a coma. In Section 3.2.4, we illustrate the access control gains a user receives due to role reassignments

The hospital nurse will not have access to the patient's PII located in the insulin pump or web server under normal conditions. However, the hospital nurse may need to update the information in the same fashion as the physician, should the patient fail into a coma. She may need to read the PII on the insulin pump given the remaining impediments. However, the hospital nurse will only have reader access to the patient's PII, located on the web server, if the patient is in a coma or if the hospital is under a code red.



The hospital technical support has the same access as the hospital nurse, only from the web server.

Finally and conversely to the web technical support, the patient's online pharmacist has reader access to the patient's PII on the web site as long as the web server does not fail.

### **3.2.4 Role Re-assignments**

Now we need to consider role changes due to various failure types. Let's take a look at the patient, Web Server Global Support, Physician's Assistant, and Nurse roles.

#### ***3.2.4.1 Assignment to the Patient Role***

Jane is Bob's spouse and Bob is the patient. We could set up a new role called "spouse" with a set of accesses and assign Jane that role or we could allow Jane to assume the role of patient as described in the IS-RBAC model under certain conditions. One feasible situation in which this may occur is when Bob becomes incapacitated (e.g., user failureR40.222) and can no longer express the password. Jane would then assume the role of the patient with the elevated accesses and privileges.

#### ***3.2.4.2 Assignment to the Web Server Global Support Role***

Reese assumes the role of the Web Server Technical Support role. Leslie assumes the Web Server Global Support role. If the patient falls into a diabetic coma or the insulin pump gets clogged, Reese's role remains unchanged. However, let's assume Leslie does not know how to handle the web server failure where it becomes overloaded, such as in a SYN-ACK distributed denial of service attack. Since Reese understands how to address this particular issue, Leslie assigns Reese the Web Server Global Support role in order to handle the situation. Right or wrong, Reese would gain elevated privileges, specifically CDRU of the PII of the patient on the web server, when Reese normally has R (reader) access.

#### **3.2.4.3 *Assignment to the Physician's Assistant Role***

Angle is a Hospital Nurse. When the patient's insulin pump becomes clogged, Jessie, the physician's assistant may assign Jessie's own role to Angel in order to facilitate repairs of the insulin pump. In this situation, Angle gains CDRU (full) access to the patient's PII located in the insulin pump when normally, Angle only has R (reader) access.

#### **3.2.4.4 *Assignment to the Nurse Role***

Rob is a paramedic and Angel is a nurse. As a nurse, Angel may only read PII from the patient's insulin pump or from the web server when the patient is incapacitated. However, when an environmental situation occurs, such as when the hospital adopts a code red circumstance, Angle may advocate for paramedic Rob to be assigned the Nurse role (assuming Rob is at the hospital). Under this role change, Rob gains no additional access to the patient's PII on the web server. However, notice that should the patient fall into a coma, Rob would gain the additional U (update) access to the patient's PII located on the insulin pump when before the environmental situation and patient's coma Rob only had R(reader) access.

#### **3.2.5 Threat Mitigation**

Without IS-RBAC, the RBAC model represents user role access controls under normal operating conditions. Should a user be reassigned to another role, the RBAC model represents the accesses the user will inherit and follows the principle of least privilege. Doing so strengthens the weaknesses caused (only) by user role changes to the protection of the Patient's PII and helps prevent potential harm to the patient.

For example, Table 5 and Table 7 indicate that under normal conditions the Hospital Nurse has no access to the patient's PII located on the insulin pump or the web site. Should the user be reassigned the role of the Physician's Assistant, the user would gain full CDRU access to the patient's PII on the insulin pump and would gain R (reader) access to the patient's PII on the

web site. Again, the RBAC model sufficiently represents this change in access controls, but only under normal conditions.

The application of the IS-RBAC model allows instrument and user failures and environmental situations to be represented so that additional access controls can be applied. Doing so follows the principle of least privilege. It also strengthens the weaknesses caused to the protection of the Patient's PII by user and instrument failures and environmental situations, mitigates threats from users with elevated user role privileges, and ultimately helps prevent potential harm to the Patient.

Let's take a look at the changes made to the access controls for the Hospital Nurse, Web Server Global Support, and the Web Server Technical Support roles. For the Hospital Nurse role, in Table 4 we see that under any adverse condition, the user gains full CDRU access. Once IS-RBAC is applied, we see from Table 6 that the user access is reduced to just R (reader) access for the insulin pump clogged tube, RU (reader update) access for when the patient suffers a coma, and R (reader) access when the Hospital enters a Code Red situation; a substantial reduction in access. This change protects the patient's PII such that the Hospital Nurse can no longer affect the availability of the data and has limited ability to potentially affect the integrity of the data.

For the Web Server Global Support and Web Server Technical Support roles, in Table 5 we see that the web server overload condition allows for full CDRU access. After IS-RBAC is applied, as shown in Table 6, their access are reduced to just R (reader). This change protects the patient's PII such that the support users can no longer affect the availability or integrity of the data.

### **3.2.6 IS-RBAC Example Definitions**

Now we can take the IS-RBAC information described in the previous section and illustrate it using the IS-RBAC definitions.

The set U of users:

$$U = \{Bob, Jane, Dakota, Jessie, Bert, Reese, Leslie, Angel, Parker, Taylor, Rob, Skyler\}$$

The set R of roles:

$$R = \{Patient, Physician, Physician's Assistant, Employer, Web Server Global Support, Web Server Technical Support, Hospital Nurse, Hospital Technical Support, Patient's Online Pharmacist, Paramedic, Ambulance Driver\}$$

A set P of permissions:

$$P = \{C (create), R (read), U (update), D (delete)\}$$

A set D of data:

$$D = \{ Bob, 15-January-1990, AZ896745, 123 Main Street Anytown USA, Gestational Diabetes, Glynase, 20 mg, myWeakPassword \}$$

A condition language LC.

A set I of instruments

$$I = \{insulin pump, web server\}$$

A set S of operational states

$$S = \{normal, overloaded, clogged tube, "Coma scale, best verbal response, incomprehensible words (R40.222)" \}$$

A set E of environmental situations.

$$E = \{Normal, Hospital Code Red\}$$

$M = \text{Instrument Availability States} \subseteq I X S$ , a many-to-many mapping instrument to operational state assignment relation.

$M = \{insulin\ pump:normal, insulin\ pump:clogged\ tube, web\ server:normal, web\ server:overloaded\}$

$Y = \text{User Availability States} \subseteq U X S$ , a many-to-many mapping user to operational state assignment relation.

$Y = \{Bob:normal, Bob:"\ Coma\ scale, best\ verbal\ response, incomprehensible\ words\ (R40.222)"\}$ , for brevity the rest of the users are associated with the normal state}

$Z = \text{User Availability States} \subseteq U X E$ , a many-to-many user to environmental situation assignment relation.

$Z = \{Rob: normal, Rob: Hospital\ Code\ Red\}$

The set of Instrument Availability Sensitive Data

$D' = \{(d,\mu) \mid d \in D, \mu \in M\}$

Table 8 shows that when instruments fail, only specific information may be available. The permissions for each data element will be assigned later, therefore this table and the two that follow contain X's to indicate the overall data field availability. For example, when the insulin pump suffers a clogged tube, the device could be programmed to display only the medication and the dosage. This will assist the patient and technician with repairs or replacement without having to navigate through the device menu screens. Similarly, when the web server becomes overloaded, it too could be programmed to provide only the most critical information in order to reduce the amount of information processed and maximize server performance.

Table 8. Data sensitivities to instrument failures.

	insulin pump: normal	insulin pump: clogged tube	web server: normal	web server: overloaded
Bob	X		X	
15-January-1990	X		X	X
AZ896745	X		X	X
123 Main Street Anytown USA	X		X	
Gestational Diabetes	X		X	X
Glynase	X	X	X	X
20 mg	X	X	X	X
myWeakPassword	X		X	

The set of User Availability Sensitive Data

$$D'' = \{(d, v) \mid d \in D, v \in Y\}$$

Table 9 clearly suggests that when the patient Bob suffers from any condition in which a physician observes he is in a form of a coma with incomprehensible verbal responses, that he will not be able to provide the password information.

Table 9. Data sensitivities to user failure.

	Bob:normal	Bob:” Coma scale, best verbal response, incomprehensible words (R40.222)”
Bob	X	X
15-January-1990	X	X
AZ896745	X	X
123 Main Street Anytown USA	X	X
Gestational Diabetes	X	X
Glynase	X	X
20 mg	X	X
myWeakPassword	X	

The set of all Availability Sensitive Data

$$D''' \subseteq \{D' \cup D''\}$$

The result of this equation is the combined columns of Table 8 and Table 9 as shown in Table 10.

Table 10. Data sensitivities to Impediments.

Data	Bob, insulin pump, web server: normal	Impediments		
		insulin pump: clogged tube	web server: overloaded	Bob:" Coma scale, best verbal response, incomprehensible words (R40.222)"
Bob	X			X
15-January-1990	X		X	X
AZ896745	X		X	X
123 Main Street Anytown USA	X			X
Gestational Diabetes	X		X	X
Glynase	X	X	X	X
20 mg	X	X	X	X
myWeakPassword	X			

$IDP = \{(u, i, d, p, c) \mid u \in U, i \in I, d \in D''', p \in P, c \text{ is an expression of } LC\}$ , The set of Impediment-sensitive Data Permissions

The easiest method to depict this information is to create a summary table based on the information from Table 10 and include the permissions associated with the data sensitivities to impediments. Essentially, if the data is available on the devices or from the patient Bob, then the information includes all of the permissions CDRU. Otherwise, none of the permissions are available, with the exception when the insulin pump has a clogged tube. In this situation, user roles will only be able to read the medication and dosage for the patient located on the insulin pump.

A partial computation of IPD illustrates how Table 11 is generated.

```

IDP = {
Insulin pump:
  Impediments = Null then
    Bob:CDRU and 15-January-1990:CDRU and AZ896745:CDRU and 123 Main
    Street Anytown USA:CDRU and Gestational Diabetes:CDRU and
    Glynase:CDRU and 20 mg:CDRU and myWeakPassword:CDRU ;
  Impediment = insulin pump:clogged tube then
    Glynase:R and 20 mg:R;
  ...
Web server:
  Impediments = Null then
    Bob:CDRU and 15-January-1990:CDRU and AZ896745:CDRU and 123 Main
    Street Anytown USA:CDRU and Gestational Diabetes:CDRU and
    Glynase:CDRU and 20 mg:CDRU and myWeakPassword:CDRU ;
  Impediment = insulin pump:clogged tube then
    Bob:CDRU and 15-January-1990:CDRU and AZ896745:CDRU and 123 Main
    Street Anytown USA:CDRU and Gestational Diabetes:CDRU and
    Glynase:CDRU and 20 mg:CDRU and myWeakPassword:CDRU;
  ...
Bob:
  Impediments = Null then
    myWeakPassword:CDRU;
  Impediment = insulin pump:clogged tube then
    myWeakPassword:CDRU;
  ...
}

```



Table 11. IDP: Data sensitivities to Impediments and associated permissions; per data source.

Data	Bob, insulin pump, web server: normal	Impediments		
		insulin pump: clogged tube	web server: overloaded	Bob:” Coma scale, best verbal response, incomprehensible words (R40.222)”
Bob	CDRU			CDRU
15-January-1990	CDRU		CDRU	CDRU
AZ896745	CDRU		CDRU	CDRU
123 Main Street Anytown USA	CDRU			CDRU
Gestational Diabetes	CDRU		CDRU	CDRU
Glynase	CDRU	R	CDRU	CDRU
20 mg	CDRU	R	CDRU	CDRU
myWeakPassword	CDRU			

NOTE: the grayed cells will be used as a sample session.

$IDPA \subseteq R \times IDP$ , Impediment-sensitive Data permission Assignment, a many-to-many impediment-sensitive data permission to role assignment relation.

The easiest method to depict this information has already been provided earlier in Table 6 and Table 7. These two tables clearly depict which roles have authorized accesses to data. When combined with the IPD provided in Table 11, a complete IPDA emerges. A partial computation of IPDA is shown below.

IDPA = {

Physician’s Assistant:

Insulin pump:

Impediments = Null then

Bob:CDRU and 15-January-1990:CDRU and AZ896745:CDRU and 123 Main Street Anytown USA:CDRU and Gestational Diabetes:CDRU and Glynase:CDRU and 20 mg:CDRU and myWeakPassword:CDRU ;

Impediment = insulin pump:clogged tube then

Glynase:R and 20 mg:R;

...

Web server:

Impediments = Null then

```

    Bob:CDRU and 15-January-1990:CDRU and AZ896745:CDRU and 123
    Main Street Anytown USA:CDRU and Gestational Diabetes:CDRU and
    Glynase:CDRU and 20 mg:CDRU and myWeakPassword:CDRU ;
    Impediment = insulin pump:clogged tube then
    Bob:CDRU and 15-January-1990:CDRU and AZ896745:CDRU and 123
    Main Street Anytown USA:CDRU and Gestational Diabetes:CDRU and
    Glynase:CDRU and 20 mg:CDRU and myWeakPassword:CDRU;
    ...
    Bob:
    Impediments = Null then
    myWeakPassword:CDRU;
    Impediment = insulin pump:clogged tube then
    myWeakPassword:CDRU;
    ...
    Hospital Nurse:
    Insulin Pump:
    Impediments = Null then
    Null ;
    Impediment = insulin pump:clogged tube then
    Glynase:R and 20 mg:R;
    ...
    Web server:
    Impediments = Null then
    Null ;
    Impediment = insulin pump:clogged tube then
    Null;
    ...
    Bob:
    Impediments = Null then
    null;
    Impediment = insulin pump:clogged tube then
    null;
    ...
    ... }

```

The set of User Availability Sensitive User role assignment

$UA' \subseteq YXR$ , a many-to-many mapping user availability states to role assignment relation.

Table 12 shows that one person who normally serves no role in this system, Bob's spouse Jane, assumes the role of the patient for the purpose of information control in the situation where Bob suffers a diabetic coma. The remainder of the user role assignments does not change under this condition.

Table 12. User role assignments with sensitivity to user failure.

Roles	Bob:normal	Bob:" Coma scale, best verbal response, incomprehensible words (R40.222)"
Patient	Bob	Bob, <b>Jane</b>
Physician	Dakota	Dakota
Physician's Assistant	Jessie	Jessie
Employer	Bert	Bert
Web Server Global Support	Leslie	Leslie
Web Server Technical Support	Reese	Reese
Hospital Nurse	Angel	Angel
Hospital Technical Support	Parker	Parker
Patient's Online Pharmacist	Taylor	Taylor
Paramedic	Rob	Rob
Ambulance Driver	Skyler	Skyler

The set of Instrument Availability Sensitive User role assignment

$UA'' \subseteq M \times R$ , a many-to-many mapping instrument availability state to role assignment relation.

Table 13 shows how Angle and Reese, the Hospital Nurse and Web Server Technical Support personnel, respectively, gain elevated access to the patient's PII when devices fail and their roles change.

Table 13. User role assignments with sensitivity to instrument failure.

Roles	insulin pump: normal and web server: normal	insulin pump: clogged tube	web server: overloaded
Patient	Bob	Bob	Bob
Physician	Dakota	Dakota	Dakota
Physician's Assistant	Jessie	Jessie, <b><u>Angel</u></b>	Jessie
Employer	Bert	Bert	Bert
Web Server Global Support	Leslie	Leslie	Leslie, <b><u>Reese</u></b>
Web Server Technical Support	Reese	Reese	Reese
Hospital Nurse	Angel	Angel	Angel
Hospital Technical Support	Parker	Parker	Parker
Patient's Online Pharmacist	Taylor	Taylor	Taylor
Paramedic	Rob	Rob	Rob
Ambulance Driver	Skyler	Skyler	Skyler

Finally, Environmental situations may control the roles users are assigned, such as when the environmental situation in a hospital emergency room changes to a medical code red. Some users (nurses) may be required to perform duties with elevated privileges normally reserved for other users (doctors).

$UA''' \subseteq ZX R$ , a many-to-many mapping instrument availability state to role assignment relation.

Table 14 shows how Rob, the Paramedic, is assigned the role of Hospital Nurse under the environmental condition when the hospital personnel operate under a Code Red.

Table 14. User role assignments sensitive to environmental situation.

Roles	Normal	Hospital Code Red
Patient	Bob	Bob
Physician	Dakota	Dakota
Physician's Assistant	Jessie	Jessie
Employer	Bert	Bert
Web Server Global Support	Leslie	Leslie
Web Server Technical Support	Reese	Reese
Hospital Nurse	Angel	Angel, <b>Rob</b>
Hospital Technical Support	Parker	Parker
Patient's Online Pharmacist	Taylor	Taylor
Paramedic	Rob	Rob
Ambulance Driver	Skyler	Skyler

The User role assignments  $UA'$ ,  $UA''$ , and  $UA'''$  need to be combined. A simple union will accomplish this task.

$$UA'''' \subseteq \{UA' \cup UA'' \cup UA'''\}$$

The  $UA''''$  is achieved by combining Table 12, Table 13, and Table 14. The rows remain the same and all the columns are included. The result is shown in Table 15.

Table 15. Impediment sensitive user role assignments.

Roles	Bob, insulin pump, web server, environment: normal	Impediments			
		Bob:” Coma scale, best verbal response, incomprehensible words (R40.222)”	insulin pump: clogged tube	web server: overloaded	Hospital Code Red
Patient	Bob	Bob, <b>Jane</b>	Bob	Bob	Bob
Physician	Dakota	Dakota	Dakota	Dakota	Dakota
Physician’s Assistant	Jessie	Jessie	Jessie, <b>Angel</b>	Jessie	Jessie
Employer	Bert	Bert	Bert	Bert	Bert
Web Server Global Support	Leslie	Leslie	Leslie	Leslie, <b>Reese</b>	Leslie
Web Server Technical Support	Reese	Reese	Reese	Reese	Reese
Hospital Nurse	Angel	Angel	Angel	Angel	Angel, <b>Rob</b>
Hospital Technical Support	Parker	Parker	Parker	Parker	Parker
Patient’s Online Pharmacist	Taylor	Taylor	Taylor	Taylor	Taylor
Paramedic	Rob	Rob	Rob	Rob	Rob
Ambulance Driver	Skyler	Skyler	Skyler	Skyler	Skyler

NOTE: the grayed cells will be used as a sample session.

Finally, we come to the session which is the instantiation of all these previous definitions.

$user : S \rightarrow U$ , a function mapping each session  $s_i$  to the single user  $user(s_i)$  (constant for the session's lifetime), and

$roles : S \rightarrow 2^R$ , a function mapping each session  $s_i$  to a set of roles  $roles(s_i) \subseteq \{r \mid (user(s_i), r) \in UA\}$  (which can change with time) and session  $s_i$  has the (impediment sensitive data)  $permissions \cup r \in roles(s_i) \{idp \mid (idp, r) \in IDPA\}$ .

When a user initiates a session, the impediment sensitivities are instantiated, data sensitivities computed, permissions calculated, and roles assigned. If one of the impediments occurs or terminates, the user sessions, impediments, role assignments, etc. are recomputed.

Let's take two sessions from the example provided. For reference, these sessions draw the information indicated by the grayed cells in Table 6, Table 7, Table 11, and Table 15. The sessions include a small subset of the same users, roles, devices, data, etc. except in the first session, where no impediments shall exist. In the second session, we will initiate one of the impediment scenarios. The result of each session is an Impediment Sensitive table that describes the role, user assignments, and authorized accesses to specific data on specific instruments.

In the first session, Jessie is the Physician's Assistant and Angel is a hospital nurse. In general, the PII on both the insulin pump and the web server may be CDRU'ed since all the PII is available. Jessie is authorized to CDRU all of the patient's PII on the insulin pump but may only R (read) the same information from the web server. Angel however, is not authorized to any of the patient's PII on the instrument or web server.

Table 16. Impediment free session.

Roles	User Role Assignment UA	Authorized to patient PII located on the insulin pump or web server
Physician's Assistant	Jessie	CDRU all data: insulin pump R all data: web server
Hospital Nurse	Angel	

Now let's introduce an impediment scenario, specifically the clogged tube on the insulin pump. As summarized in Table 17, the authorized access is R (read) for all data for both Jessie and Angel. However, the impediment sensitive data allows only the medication and dosage to be accessed from the insulin pump. Regardless, all of the information may be read from the web server. For Angel, this constitutes a significant gain in access to the patient's PII. Angel rose from no access to the ability to read all of the patient's PII.

Table 17. Clogged tube on the insulin pump session.

Roles	User Role Assignment UA''''	Authorized to patient PII located on the insulin pump or web server
Physician's Assistant	Jessie and Angel	R all; only available data: medication & dosage; insulin pump R all; available data: all; web server
Hospital Nurse	Angel	R all; only available data: medication & dosage; insulin pump

### 3.3 Summary

This section presented the IS-RBAC model. Five new definitions were added to the standard RBAC model in order to represent instrument and user failures and environmental situations. With RBAC, the unanticipated role accesses were shown to negatively impact the confidentiality, availability, and integrity of the Patient's PII. These impacts weaken data protections, expose the data to threat actors, and potentially harm the privacy or even safety of the Patient.

The IS-RBAC model was applied to the example scenario user role assignments with authorized role accesses in a Socio-Technical System. Role reassignments were discussed and



modeled for a set of four impediments. The IS-RBAC model allows the impediments to be represented so that additional access controls can be applied. Doing so strengthens the weaknesses caused to the protection of the Patient's PII by user and instrument failures and environmental situations, mitigates threats from users with elevated user role privileges, and ultimately helps prevent potential harm to the Patient.

The next section discusses the conclusions made from this thesis. Also presented are some ideas for future work on the IS-RBAC model.

## 4 Conclusions

In this thesis, a variation of the standard RBAC model, termed an Impediment Sensitive Role-Based Access Control (IS-RBAC), was developed. IS-RBAC represents the sensitivities to data availability and user role assignments that instrument and user failures and environmental situations have on Socio-Technical Systems. We added five definitions to the standard RBAC model to generate the new IS-RBAC model.

This thesis discusses the differences in the granularity between how the standard RBAC model and the new IS-RBAC model represent data, impediments, user role assignments and access controls. Specifically, the application of the IS-RBAC model allows instrument and user failures and environmental situations to be represented so that additional access controls can be applied. It also strengthens the weaknesses caused to the protection of the Patient's PII by user and instrument failures and environmental situations, mitigates threats from users with elevated user role privileges, and ultimately helps prevent potential harm to the Patient. IS-RBAC follows the principle of least privilege.

To demonstrate the feasibility of the IS-RBAC model, we examined a number of embedded or closely worn medical devices. These devices along with the patient, physician, and other actors were presented as examples of Socio-Technical Systems. IS-RBAC was then applied to an example Socio-Technical System which consisted of an insulin pump, web server, patient, PII, and a variety of additional user roles. We used an established dependability and security taxonomy that classifies instrument failures and an internationally accepted medical taxonomy that classifies user failures. We discussed several types of environmental situations which were also shown to impede user role assignments and data availability. Based on these taxonomies and example environmental situations we enumerated four impediments. These impediments were applied to the definitions of the IS-RBAC model as an example scenario in order to represent new user role assignments and data availability for the Socio-Technical System.

The IS-RBAC model contributes to an associative relationship between the availability and the confidentiality properties of a system. By definition, the information in a system must be available when needed. We have illustrated and demonstrated that impediments from instruments, users, and environment affect both the availability of data and user role assignments.

While RBAC can represent users and roles, IS-RBAC can further represent instruments, data, failures, and environmental situations. While RBAC can represent user role assignments and permissions, IS-RBAC can further represent these same user role assignments and permissions under variable data availability conditions when instruments and users fail and when environmental situations change. RBAC allows user role assignments to change during an established session and thus mitigates the threat from users gaining unauthorized access to data. IS-RBAC capitalizes on this feature so that when a user role changes, unauthorized access to data is mitigated, under additional conditions, when instruments and users fail and when environmental situations change.

## 5 Future work

It seems feasible that one could use portions or the entire IS-RBAC model with additional definitions found in other RBAC models. For example, the user role assignment,  $UA$ , found in Q. Ni's [2] Core P-RBAC model, might be directly substituted with the definition of  $UA''''$  in the IS-RBAC model. The benefit of doing so would allow the impediments modeled in IS-RBAC to be included in the Core P-RBAC model and its subsequent applications. Such a combination of RBAC modeling may yield an even more comprehensive solution to a wider variety of real world conditions and solve a greater number of INFOSEC requirements.

The Laprie's taxonomy of Dependability was used to enumerate impediments for the IS-RBAC model. How much more of the Dependability model can be merged into RBAC in a similar fashion? For example, Laprie's Dependability and Security taxonomy shown in Figure 7 depicts the "means" by which a system is rendered dependable. Specifically, by modeling preventions, tolerance, removal, and forecasting, it may be possible to including these dimensions into some form of RBAC. By continuing along this line of model combination one may eventually define a Dependability Sensitive RBAC. Conversely, one could examine whether any of the existing derivations of the RBAC model already contain elements in Laprie's taxonomy of Dependability. For example, in Laprie's Dependability and Security taxonomy, "attributes" of a Dependability and Security model include well established INFOSEC concepts of Availability, Confidentiality, and Integrity. An understanding of how those aspects are represented in an RBAC model may prove useful in defining a Dependability and RBAC Security model.

What does a session mean in a Socio-Technical System? A session in the original RBAC applies to a single Technical Computer-Based System. Since a Socio-Technical System is composed of multiple Technical Computer-Based Systems, it stands to reason that to represent a session in a Socio-Technical System requires another dimension. Instead of session  $s_i$ , where  $i$  represents a single session instance, we need session  $s_{ij}$ , where  $j$  represents the instantiation of a

set of multiple Technical Computer-Based Systems. This modification may allow multiple RBAC modeled systems join into a Socio-Technical System.

The IS-RBAC model was designed for a Socio-Technical System. Could it be used for a single Technical Computer-Based System? It seems feasible to do so if we drop all impediments except for those associated with a single Technical Computer-Based System. The result would be an IS-RBAC without concern for user failures or environmental situations. The faults of the single system could be enumerated and used to define user role assignments and data availability. Essentially, it would remove all columns (dimensions) of impediments listed in the tables of Section 3 except for those associated with a single instrument. Likewise, the user failings could be disposed of or if not needed, removed from enumeration. The result would be an IS-RBAC based on just a set of unified Technical Computer-Based System which could be viewed as a monolithic system.

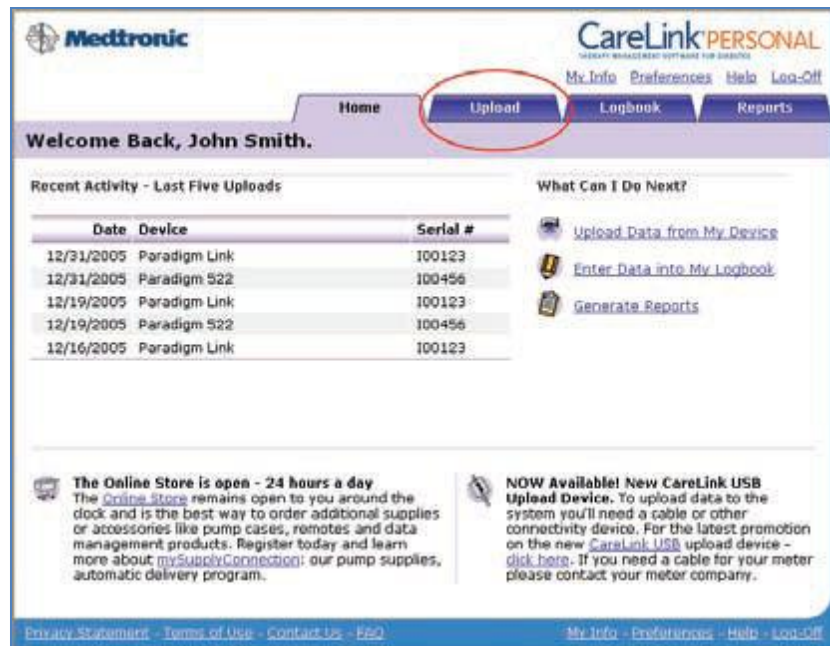
## 6 Appendix A: Additional Embedded or Closely Worn Medical Devices

### Devices

This appendix continues the discussion of implanted or closely worn medical devices from Section 2.2.

#### 6.1 Insulin Pump: CareLink Website

The type of information stored in the CareLink website is shown in Figure 12 and Figure 13 below. Here we see the user name and the date of recent data uploads. The data uploads include blood glucose and sensor glucose levels, and insulin infusions. Data reports as shown in Figure 14 can also be printed and emailed to user's outside the boundary of the Socio-Technical System.



The screenshot shows the CareLink Personal website interface. At the top left is the Medtronic logo. At the top right is the CareLink PERSONAL logo with the tagline 'HEALTH MANAGEMENT SOFTWARE FOR DIABETES'. Below the logo is a navigation bar with links for 'My Info', 'Preferences', 'Help', and 'Log-Off'. A secondary navigation bar contains 'Home', 'Upload', 'Logbook', and 'Reports', with 'Upload' circled in red. Below the navigation is a welcome message: 'Welcome Back, John Smith.' The main content area is divided into two columns. The left column is titled 'Recent Activity - Last Five Uploads' and contains a table with the following data:

Date	Device	Serial #
12/31/2005	Paradigm Link	100123
12/31/2005	Paradigm 522	100456
12/19/2005	Paradigm Link	100123
12/19/2005	Paradigm 522	100456
12/16/2005	Paradigm Link	100123

The right column is titled 'What Can I Do Next?' and contains three links: 'Upload Data from My Device', 'Enter Data into My Logbook', and 'Generate Reports'. At the bottom of the page, there are two promotional banners. The left banner is titled 'The Online Store is open - 24 hours a day' and describes the store's availability and products. The right banner is titled 'NOW Available! New CareLink USB Upload Device' and describes the new device and its features. The footer contains links for 'Privacy Statement', 'Terms of Use', 'Contact Us', 'ESQ', and 'My Info - Preferences - Help - Log-Off'.

Figure 12. User information (e.g., PII) on the CareLink website.



**CareLink PERSONAL**  
THErapy MANAgEMENT SOFTWARE FOR DIABETES  
[My Info](#) [Preferences](#) [Help](#) [Log-Off](#)

Home
Upload
Logbook
Reports

**Logbook for May 4, 2007**

Time	Entry	Comment	Edit	Delete
1:25 AM	Exercise: 30 minutes at Low intensity	Went jogging		
7:25 AM	Carbohydrate: 25 grams	Small carbs		

[Privacy Statement](#) - [Terms of Use](#) - [Contact Us](#) - [FAQ](#)

[My Info](#) [Log-Off](#)

--Select--  
 --Select--  
 Carbs  
 Exercise  
 HbA1c  
 Infusion Set Change  
 Urine Ketones

Figure 13. Logbook entry on the CareLink website.

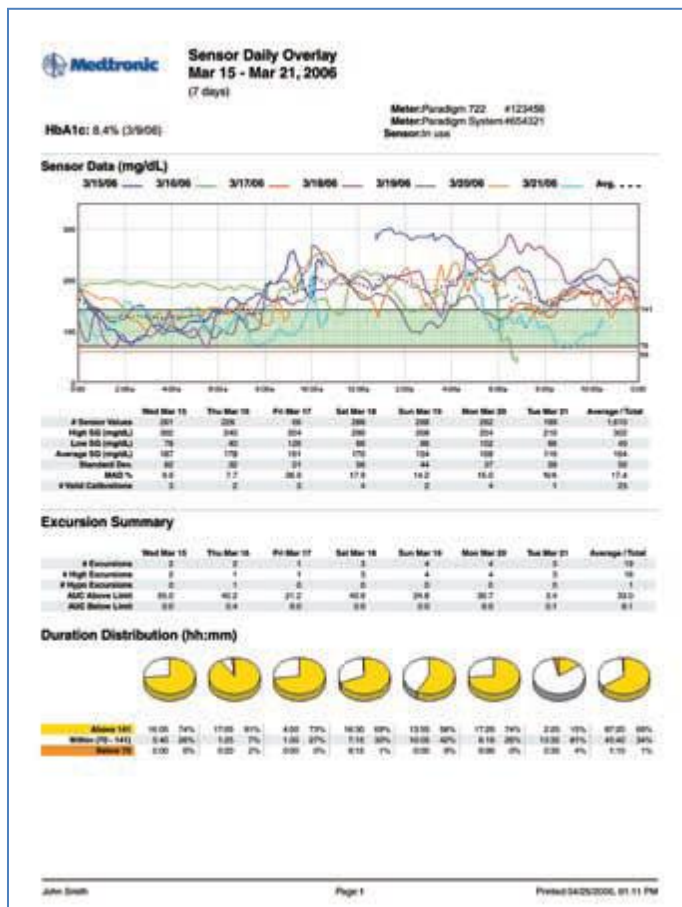


Figure 14. PII and medical information on the CareLink website.

## 6.2 Pacemaker

Figure 15 depicts the placement of an implanted pacemaker in the human body.

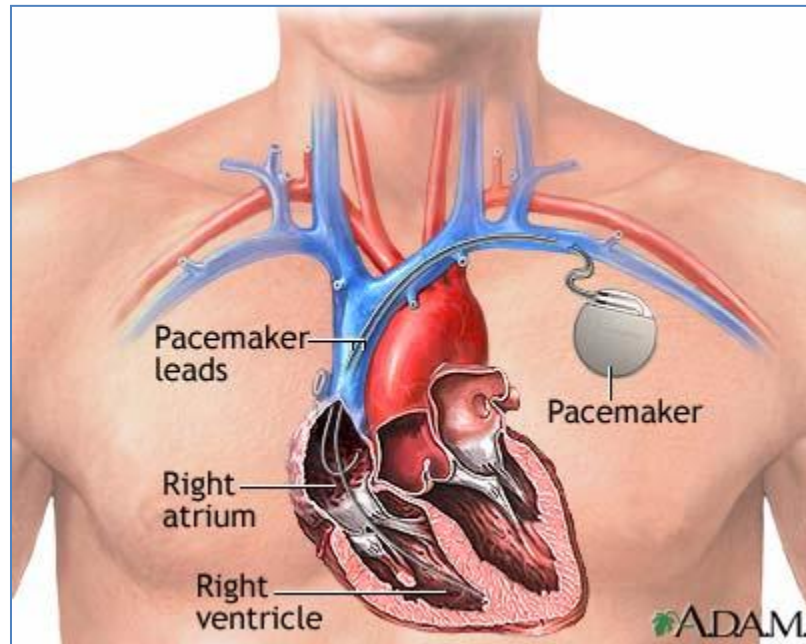


Figure 15. A pacemaker placement.

## 6.3 Hearing Aid

The Siemens “Pure” hearing aid shown in Figure 16 also includes two sizes of Bluetooth remote controls as shown further in Figure 17 and Figure 18.





Figure 16. Siemens Pure hearing aid.



Figure 17. Siemens Pure hearing aid with Bluetooth remote control.

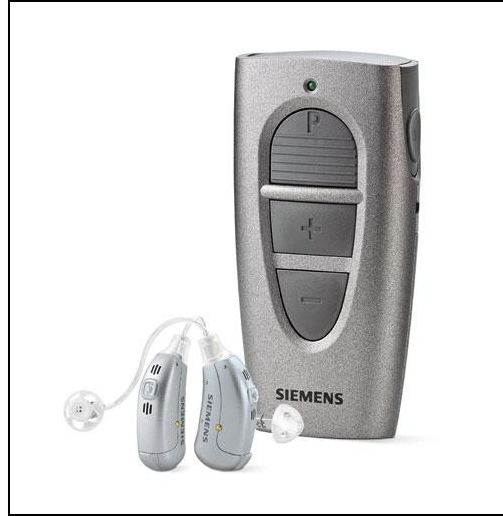


Figure 18. Siemes Pure hearing aid with pocket remote control.

Access to information stored in the devices is performed via a wired interface or a wireless Bluetooth interface and software from the manufacturer. Siemens’ “Connexx” software “...uses the power of your PC to give you additional precision when fitting Siemens advanced technology programmable hearing instruments.”[41] The software is available only for licensed hearing professionals or for clinical studies through a “mySiemens” account (or for creative users at software sharing websites) and required interface hardware can be purchased on eBay.

It is important to note that “no PII is stored in the [hearing aid] device, only the programming necessary for the device and the serial number assigned to the device.”[42] PII is stored in a centralized (perhaps the “cloud”?) database separate from the device and used by technicians and their administration PCs for configuring devices. From a single Technical Computer-Based System perspective, confidentiality of PII remains a non-issue for this device. However, the device is part of a larger Socio-Technical System including the Bluetooth remote controller, the user’s Bluetooth enabled smartphone, the user’s Bluetooth enabled audio system (TV, MP3 player, etc.), the technician’s programming workstation, and the technicians’ centralized database server.

The hearing aid device limits PII exposure to a user's computing environment by not including identity information such as name, SS#, address, email, etc. A simple enough approach, however, the devices do retain a serial number that associates the device and the information stored within, to the user information stored in a networked computing environment. Since the devices store a large amount of medical information and can be connected to networks, and contain a reference number that links the user to the PII, we must expand the definition of the simple hearing aids devices to include all these interacting elements.

Like the insulin pump Socio-Technical System described earlier, the users and other actors include the user of the hearing aid, the administrators of the technician's Internet Service Provider, the administrators of the Internet server and Connexx website, and the additional consumers of the user's information such as the nurses, doctors, and administrators of the doctor's computer systems.

Within the confines of a widely defined Socio-Technical System, a malicious user might be able to access PII via the serial number that provides a direct key index to the PII stored in the database. Additionally, data integrity remains an issue since a malicious user could potentially change a serial number and obtain unauthorized access to the necessary programming for another user.

The environments in which the hearing aids operate are very similar to the insulin pump presented earlier. However, a major component is absent in the hearing aid Socio-Technical System, namely, the user's PC. Instead, the technician's PC is required to transfer user data across the Internet to a centralized computer. Regardless, nature of the operational environments remains similar.

## 6.4 H'andy Sana 210

The H'andy sana[43] 210 is a mobile phone that includes an application called “Heart Suite”, see Figure 19 and Figure 20 below. Technically, this device is not imbedded in the user or connected via wires or wireless network. Instead, it measures a user’s Electrocardiogram (ECG) by putting two fingers on the sensor field of the H'andy sana 210. Thus, the connection from the user to the device is temporary and controlled by the user. This instrument operates in the same types of environments as other instruments presented above. It allows a user to take their ECG instantly from anyplace and send it to the hospital or doctor for interpretation. H'andy sana 210 has a 2.8 inch full touch screen and full-fledged mobile phone capabilities including multimedia suite, Internet browser, calendar, built-in camera with screen viewfinder and dedicated menus. It offers online health suite services to store data like blood pressure, cholesterol, blood glucose, and ECG monitor results.



Figure 19. The H'andy Sana 210 with “Heart Suite” ECG phone.



Figure 20. The H'andy Sana 210. Placing fingers on the sensors.

## 6.5 ICE: In Case of Emergency Application

Appventive provides an “In Case of Emergency” (ICE) application[44] for the Android smartphone. A user enters the following information which can be easily retrieved by “first responders”:

- A list of people to call -- can call directly from the app
- Insurance information
- Primary doctor's name and number -- can call directly from the app
- Allergies
- Medical Conditions
- Medications
- Any special instructions or other information you wish to provide

Figure 21 depicts the user owner information stored in the ICE application. This application is fashioned after the old fashioned commonplace medical alert bracelets/necklaces. Under normal operating conditions, “first responder” users do not access PII because the owner user typically controls content with physical restraint. However, it

is expected that should the owner user become incapacitated (a user “failure”), the first responder user will be authorized to retrieve the information.

The environment of this application appears limited to the user’s smartphone. However, users may provide first responders or medical personnel with physical control of the device. At that point, the environment in which the device operates expands to any other Technical Computer-Based System or actors that the new actor operates.

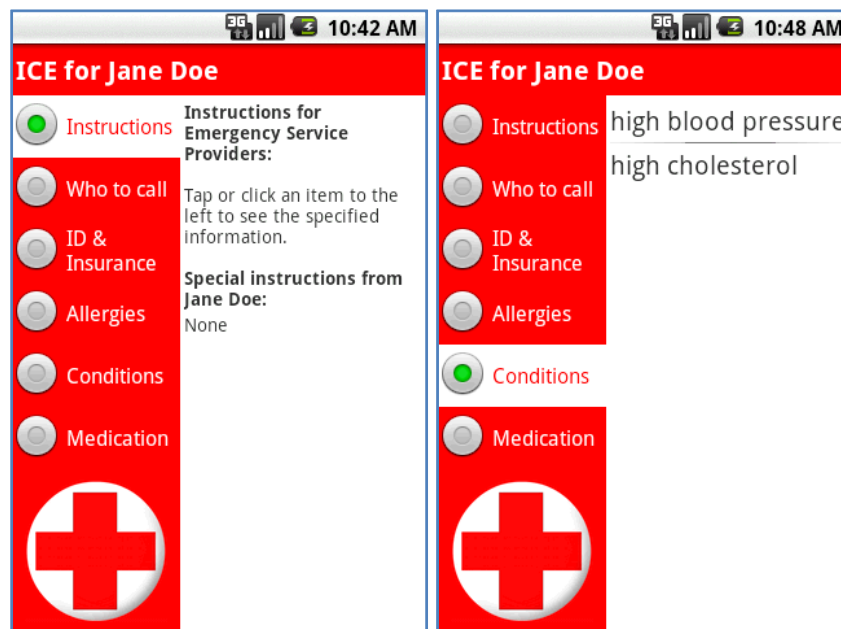


Figure 21. Sample ICE screen shots.

## 6.6 Heart Rate Monitor

SportsTrackLive offers the Zephyr heart rate monitor, a bioharness, and an Android smartphone application. The Zephyr Bioharness module monitors a user’s heart rate, breathing rate, and skin temperature. The Zephyr HxM module showed in Figure 22 monitors heart rate and cadence. The Sports Tracker Pro application software on the smartphone incorporates the user’s location, speed, and distance into an integrated interface as shown in Figure 23 below.

This technology combines specialized monitoring devices with a smartphone. The environment for this system includes transfer and storage across the Internet. The information stored in the smartphone can also be automatically (or manually) uploaded to a share webspace at <http://www.sportstracklive.com/> as shown further in Figure 24. Here we see the speed altitude, distance duration, timestamp, and identity of three users. Detailed information about a user's exercise experience can be selected and displayed as shown in Figure 25 and Figure 26. In this Internet environment, specific users can also be searched/filtered in the website.

Personal Note: While this author uses the HxM BT module and SportTrackPro software on a DroidX smartphone, I chose not to participate in the live data uploads.



Figure 22. The HxM™ BT module (device with Zepher written on it) and the Zephyr Bioharness for monitoring a person's heart rate, speed, and distance.



Figure 23. The SportTrackLive application on an Android smartphone.



Figure 24. Live user monitoring data uploaded to shared website <http://www.sporttracklive.com/>.



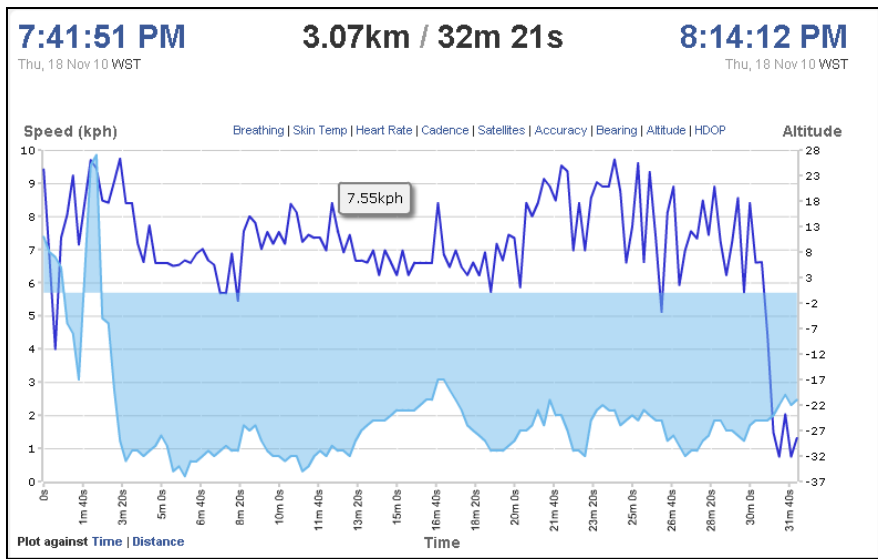


Figure 25. Detailed information from Live user monitoring.

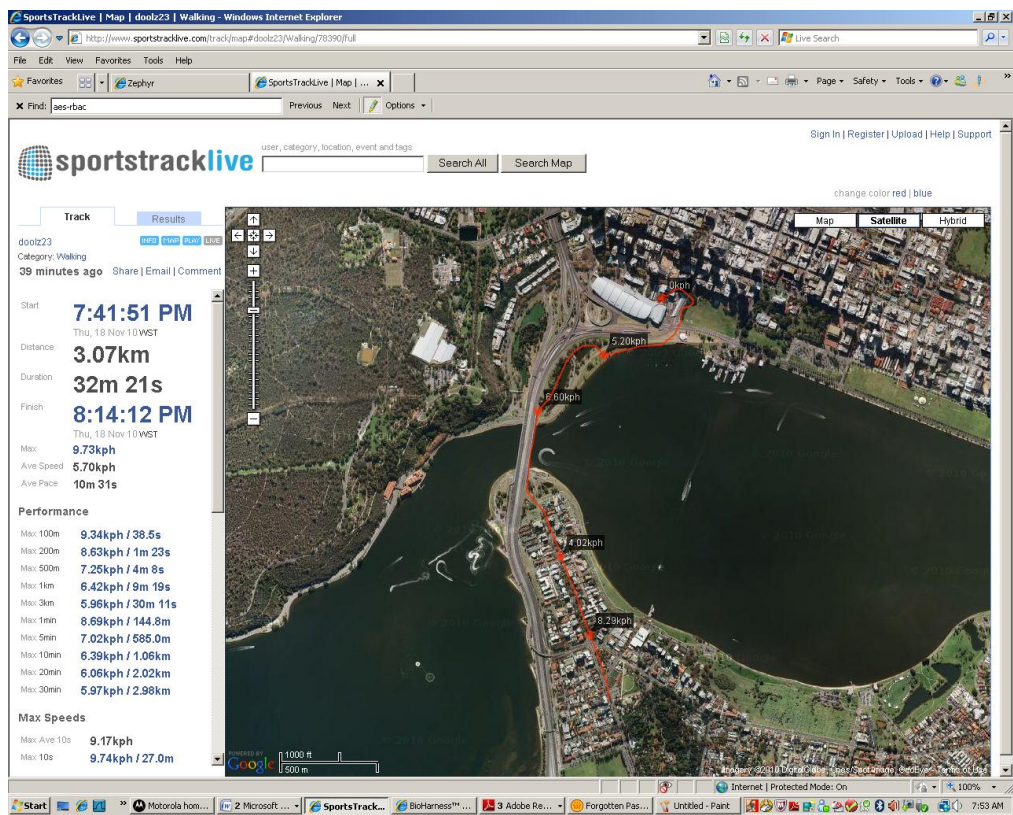


Figure 26. Detailed location from Live user monitoring.

## 6.7 ICE Medical ID Card

Like the ICE application discussed above, Memitech offers a USB storage device that retains the same information and an application. The form factor is a plastic card the size and thickness of a credit card. The USB storage flips out of the card and is then inserted into a computer USB port as shown in Figure 27 and Figure 28. The software application launches automatically if Autorun feature is enabled, otherwise a user must run the application from the storage location. Once initiated, the software will display PII for the user owner as shown in Figure 29.

Like the ICE application discussed earlier, under normal operating conditions, “first responder” users do not access PII because the owner user typically controls content contained on the device with physical restraint. However, given the Internet environment, it is expected that should the owner user become incapacitated (a user “failure”), the first responder user will be authorized to retrieve the information, assuming they possess a personal computer. Like the ICE application discussed above, once the device is physically distributed to another actor, the environment in which it operates automatically expands to any other Technical Computer-Based System or additional actors.



Figure 27. ICE Medical ID card. A USB thumb drive in a credit card format.



Figure 28. Pop-out the thumb drive and insert into USB port of computer.

ICE Medical ID - Joseph Frederick Blumberg - October/09/2010

**Emergency Summary** My Family Profiles My Files Print Help

To all medical personnel and medical institutions: Please treat all information on this card as confidential. I hold you harmless for all actions based on the accuracy of information on this card.

Personal Conditions Medications Allergies Doctors/Dentists Surgeries/Treatments Vaccines Insurance Family History Social History

**NAME**

Living Will Resuscitation Instructions Power Of Attorney My Medical Tests and Lab Results

Title	First	Middle	Last	Date of Birth		
Mr.	Joseph	Frederick	Blumberg	29	Jan	1959

Figure 29. Screen capture of ICE Medical ID application.

## 6.8 Cardio Trainer

WorkSmart Labs, Inc. offers Cardio Trainer[45] application for the Android smartphone. Like the Zephyr Heart Rate Monitor application discussed above, CardioTrainer tracks a user's location and speed for a variety of exercise activities as shown in Figure 30.

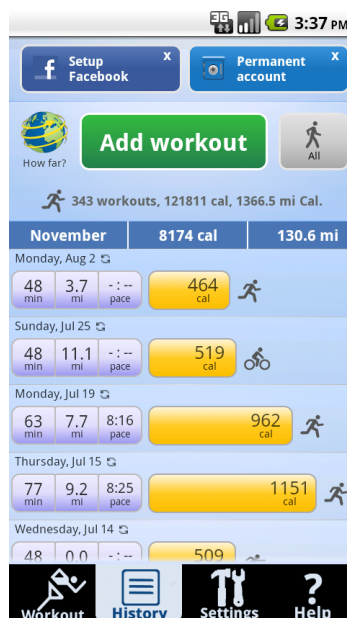


Figure 30. Cardio Trainer application on Android smartphone.

What makes CardioTrainer unique is that according to its website, "... was selected as the first partner to upload mobile fitness data to the new [Google Health] service." According to Google Health website[46], the service provides a solution to help users organize, track, monitor, and act on health information.

The new Google Health is designed to help you keep track of all of your personal health and medical information, making it easy to share very specific pieces of information with family members and health professionals. The updated design helps you keep your profile up-to-date, focusing on current activity and conditions while hiding and saving what has happened in the past. All of these changes are available immediately when you log into your Google Health account.

Figure 31 depicts user John Smith's exercise activity (calories burned over time). The data was uploaded from the Cardio Trainer application on John's Android smartphone to

WorkSmart Labs website and transferred to John’s account on the Google Health website. The figure shows John’s activity over several days. This Socio-Technical System also uploads information to Twitter.

Google Health offers optional information sharing of this data to other individuals and organizations. By selecting from a directory of “personal health services”[47], the PII is transferred to organizations’ web applications.

When you link a website to your profile, you may authorize that website to read your Google Health profile or to automatically send and update information in your profile (such as medical records or prescription histories). You decide which permissions to grant when you sign up with each website.

These organizations offer online medical services, pharmaceutical history, lower cost medication review, and personal health assessments, to name a few.

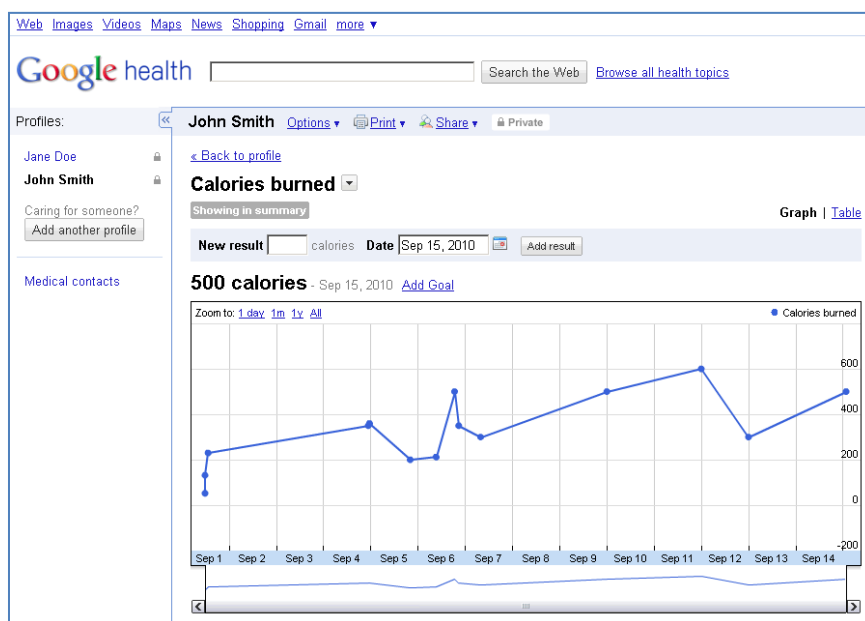


Figure 31. Cardio Trainer exercise activity uploaded and displayed on John Smith’s Google Health website.

## 6.9 Electric “Sheep”

Electric Sheep is an application that runs on the Android smartphone and requires no additional external sensors. Instead, it uses the devices accelerometers to track a user’s motion

while sleeping. Figure 32 shows a sample sleep pattern collected and displayed on the smartphone. However, the application also collects the user's sleeping information and uploads the data to Google Analytics. The application supports by default "Anonymous usage will be uploaded" feature.

This author provided the following inquiry[48] to the developer of the application.

"Anonymous usage uploaded" concerns me. What will the data be used for and who will have access?

The developer of the application responded[49] as follows:

It is uploading to google analytics. Currently only I can see this data. I'm tracking page views, so I know what parts of my app is being used, and how often- giving me a general idea of how many people are using my app on any given day, etc. Also tracked is your calibration result after you use the calibration wizard, along with some information about your accelerometer and the hardware name of the phone that is being used. I'm considering perhaps going further by tracking ratings and \*some\* general information about sleep movement, but I don't think I would want to go so far as to track anyone's whole night- too creepy.

Let me know if you have any more concerns,

Jon

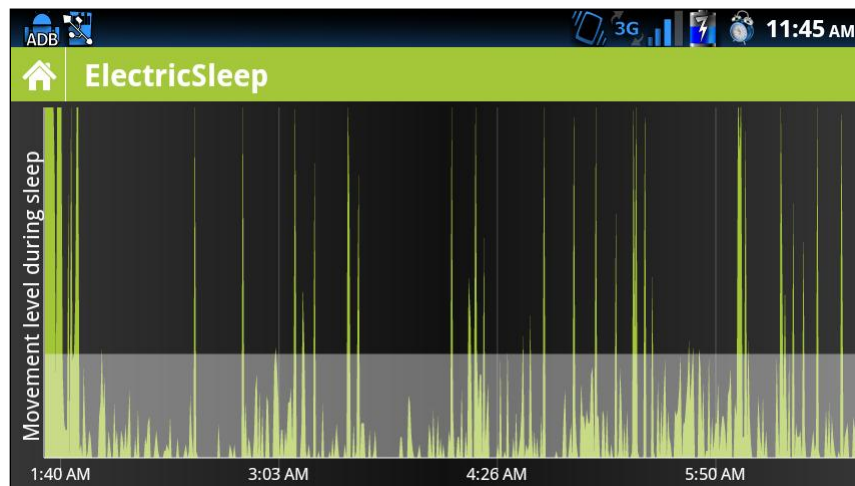


Figure 32. Movement levels detected by Electric Sheep application on Android smartphone.

## 6.10 Ultrasound

Popular Science reported on a new product called the Vscan[50] by General Electric Healthcare[51]. It provides a physician with ultrasound information in a very small form about the size of a cell phone as shown in Figure 33.

The VSCAN, “does everything that a conventional briefcase-size ultrasound computer can do. Glide the mini transducer wand over the patient, and it emits ultrasound waves that travel through the body. A computer measures the timing and magnitude of the return echoes and turns that data into a high-resolution 2-D image.”

Technically, this device is not imbedded or worn by the user. Therefore, it is not an instrument as described in this paper, but it is very close. Should the manufacturer focus on the patient instead of the physician as the user market, it is not unreasonable to visualize patients routinely conducting ultrasounds of their own bodies and sending that information to doctors and hospitals much in the same way as the H’andy Sana 210 discussed above.

It should also be noted that CNET reported the VSCAN, “--could prove profoundly useful, with battery life being the first-gen device's biggest obstacle in the world of mobile care.”[52] One might investigate how information in this device is protected if battery life becomes low.



Figure 33. The VSCAN handheld ultrasound.

## 7 Appendix B: ICD10

This appendix includes a handful of the International Classification of Diseases, Tenth Revision, Clinical Modification (ICD-10-CM)[53]. The R40 series deals with patient coma and the R45 deals with patient emotional states. Below in the list, the R40.222 is highlighted and bolded. It was used as the user impediment in the example application of the IS-RBAC model. A complete version may be found online at <http://www.cdc.gov/nchs/icd/icd10cm.htm#10update>.

### ICD-10-CM TABULAR LIST of DISEASES and INJURIES

2011Page 934

R40.2

Coma

Coma NOS

Unconsciousness NOS

Code first

any associated:

coma in fracture of skull (S02.-)

coma in intracranial injury (S06.-)

The appropriate 7th character is to be added to each code from subcategory R40.21-, R40.22-, R40.23-:

0 - unspecified time

1 - in the field [EMT or ambulance]

2 - at arrival to emergency department

3 - at hospital admission

4 - 24 hours or more after hospital admission

Note:

A code from each subcategory is required to complete the coma scale

These codes are intended primarily for trauma registry and research use but may be utilized by all users of the classification who wish to collect this information

R40.20

Unspecified coma

R40.21

Coma scale, eyes open

R40.211

Coma scale, eyes open, never

R40.212

Coma scale, eyes open, to pain

R40.213

Coma scale, eyes open, to sound

R40.214

Coma scale, eyes open, spontaneous



R40.22

Coma scale, best verbal response

R40.221

Coma scale, best verbal response, none

### **R40.222**

#### **Coma scale, best verbal response, incomprehensible words**

R40.223

Coma scale, best verbal response, inappropriate words

R40.224

Coma scale, best verbal response, confused conversation

R40.225

Coma scale, best verbal response, oriented

R40.23

Coma scale, best motor response

R40.231

Coma scale, best motor response, none

R40.232

Coma scale, best motor response, extension

R40.233

Coma scale, best motor response, abnormal

R40.234

Coma scale, best motor response, flexion withdrawal

R40.235

Coma scale, best motor response, localizes pain

R40.236

Coma scale, best motor response, obeys commands

R45

Symptoms and signs involving emotional state

R45.0

Nervousness

Nervous tension

R45.1

Restlessness and agitation

R45.2

Unhappiness

R45.3

Demoralization and apathy

Excludes1:

anhedonia (R45.84)

R45.4

Irritability and anger

R45.5

Hostility  
R45.6  
Violent behavior  
R45.7  
State of emotional shock and stress, unspecified  
R45.8  
Other symptoms and signs involving emotional state  
R45.81  
Low self-esteem  
R45.82  
Worries  
R45.83  
Excessive crying of child, adolescent or adult  
Excludes1:  
excessive crying of infant (baby) R68.11  
R45.84  
Anhedonia  
R45.85  
Homicidal and suicidal ideations  
Excludes1:  
suicide attempt (T14.91)  
R45.850  
Homicidal ideations  
R45.851  
Suicidal ideations  
R45.86  
Emotional lability  
R45.87  
Impulsiveness  
R45.89  
Other symptoms and signs involving emotional state

## 8 Appendix C: Siemens Hearing Instruments - Troubleshooting.

Siemens Hearing Instruments – Troubleshooting[54]

There are a few common situations new users may face with their hearing Instruments. These are generally easy to solve as explained in the table below.

The hearing Instrument does NOT whistle when you hold it in your hand. (Only applicable if hearing Instrument does not have an automatic feedback reduction system.)

Check: Is the hearing Instrument switched on?

Is the volume control in the right position?

Is there enough power in the battery?

Is the earmould blocked with dirt or earwax?

Have you selected the right listening program? (For example, programs designed specifically for telephone use will not allow you to hear any whistling when the Instrument is held in the hand.)

Is the hearing Instrument damaged?

The hearing Instrument whistles while your child is wearing it.

Check: Is the earmould inserted correctly?

Is the volume control in the right position?

Is there any crack in the earmould tubing or ear hook?

Is there too much earwax in your child's ear canal?

Is the earmould too small, because of physical changes in the ear canal?

Is the earmould tubing connected properly to the earmould and the hook?

Is the hook or tube damaged?

Is the child leaning against a flat surface, blocking the microphone? (E.g. infant in car seat)

The hearing Instrument is dead.

Check: Is the battery flat?

Is the battery inserted correctly?

Is the hearing Instrument turned on?

Is there any corrosion on the battery or the battery contact area?

Is the earmould blocked with earwax?

Is the earmould tubing blocked?

Are there water droplets in the ear hook?

Your child says the hearing Instrument isn't working properly.

Check: Is the volume control in the right position?

Is the opening to the microphone blocked with dirt or dust?

Is the battery flat?

Is the earmould blocked with earwax or dirt?

Is there too much earwax in your child's ear canal?

Is the hearing Instrument damaged?

Are both the hook and the tube dry?

Connect the stethoset and check if the hearing Instrument still works, and/or if you can hear unusual sounds.

The hearing Instrument generates distortion and/or unusual sounds (like crackling).

Check: Is there corrosion or rust on the battery or inside the battery compartment?

Is the battery inserted properly in its compartment?

Is the on-off switch at the correct position?

Is the volume control in the right position?

Is the earmould blocked?

Are there water droplets in the ear hook or earmould tube?

Is the earmould fitted correctly?

If the hearing Instrument comes into contact with water.

Steps: Shake the water away quickly.

Remove the battery.

Have the hearing Instrument checked by your Hearing Care Professional. If this is not possible: use your dry aid kit.

Leave the hearing Instrument in a dry place.

Connect the stethoset and check if the hearing Instrument is still working.

## Bibliography

- [1] HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996, Public Law 104-191, 104th Congress, <http://aspe.hhs.gov/admsimp/pl104191.htm>, (Accessed November 24, 2009).
- [2] Q. Ni, D. Lin, E. Bertino, and J. Lobo. Conditional privacy-aware role based access control. In J. Biskup and J. Lopez, editors. *Computer Security - ESORICS 2007*, 12th European Symposium On Research In Computer Security, Dresden, Germany, September 24-26, 2007, Proceedings, volume 4734 of Lecture Notes in Computer Science. Springer, 2007.  
<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.83.5560&rep=rep1&type=pdf>
- [3] Strembeck, M. and Neumann, G. 2004. An integrated approach to engineer and enforce context constraints in RBAC environments. *ACM Trans. Inf. Syst. Secur.* 7, 3 (Aug. 2004), 392-427. DOI= <http://doi.acm.org/10.1145/1015040.1015043>
- [4] Amirreza Masoumzadeh , James B. Joshi, PuRBAC: Purpose-Aware Role-Based Access Control, Proceedings of the OTM 2008 Confederated International Conferences, CoopIS, DOA, GADA, IS, and ODBASE 2008. Part II on On the Move to Meaningful Internet Systems, November 09-17, 2008, Monterrey, Mexico [doi>10.1007/978-3-540-88873-4\_12]
- [5] Ian Sommerville. 2006. *Software Engineering: (Update) (8th Edition) (International Computer Science)*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA.
- [6] “A Dependability Model for Domestic Systems”, Dewsbury G, Sommerville I, Clarke K, Rouncefield M (2003) A Dependability Model of Domestic Systems, in Anderson, Felici & Littlewood (Eds), *Computer Safety, Reliability And Security: 22nd International Conference, Safecomp 2003*, Proceedings, Lecture Notes In Computer Science, 2788, Heidelberg, Springer-Verlag, 103-115.  
<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.140.5936&rep=rep1&type=pdf>  
(viewed November, 2010).
- [7] Insulin Study Could Lead to New Dosage Devices, NATASHA SINGER, Published: February 4, 2010, New York Times,  
[http://www.nytimes.com/2010/02/05/business/05diabetes.html?\\_r=1](http://www.nytimes.com/2010/02/05/business/05diabetes.html?_r=1), (Viewed August, 2010).
- [8] CareLink Software, Medtronic MiniMed, Inc., <http://www.medtronic-diabetes.co.uk/product-information/carelink-personal-therapy-management-software/index.html>. (viewed November, 2010).
- [9] CareLink™ Personal software, Copyright © 2008 Medtronic MiniMed, Inc.,  
<http://www.medtronic-diabetes.co.uk/product-information/carelink-personal-therapy-management-software/index.html> (viewed October, 2010).
- [10] Pacemaker Definition, by Mayo Clinic staff,  
<http://www.mayoclinic.com/health/pacemaker/MY00276> (viewed July - November, 2010).
- [11] CareLink Remote Monitoring Network, Medtronic, Inc, 2010. (viewed November, 2010).

- [12] Home Monitoring® Applications for Cardiac Resynchronization Therapy, BIOTRONIK, <http://www.biotronik.com/en/us/4939> (viewed November 2010).
- [13] Fig. 3: Reduction of the patients heart rate variability, BIOTRONIK, 2010. [http://www.biotronik.com/en/us/2021/?template=screenshot\\_image\\_d&fullsize=true](http://www.biotronik.com/en/us/2021/?template=screenshot_image_d&fullsize=true) (viewed November, 2010).
- [14] LAZARUS, A. (2007), Remote, Wireless, Ambulatory Monitoring of Implantable Pacemakers, Cardioverter Defibrillators, and Cardiac Resynchronization Therapy Systems: Analysis of a Worldwide Database. *Pacing and Clinical Electrophysiology*, 30: S2–S12. doi: 10.1111/j.1540-8159.2007.00595.x <http://onlinelibrary.wiley.com/doi/10.1111/j.1540-8159.2007.00595.x/abstract> (viewed November, 2010).
- [15] “Instant Heart Rate”, by “Modula d.o.o.” <http://www.instantheartrate.com/> downloaded (August, 2010).
- [16] “Instant Heart Rate monitor for Android and iPhone 4”, Modula, <http://www.modula.si/instantheartrate/en> (viewed November, 2010).
- [17] Twitter feed to Modulo’s web site. © Modula d.o.o. 2010 <http://www.instantheartrate.com> (viewed December, 2010).
- [18] “Failure”, Merriam-Webster (online dictionary), <http://www.merriam-webster.com/dictionary/failure> (viewed August, 2010).
- [19] “Failure”, Dictionary.com, <http://dictionary.reference.com/browse/failure> (viewed August, 2010).
- [20] National Information Assurance (IA) Glossary, CNSS Instruction No. 4009, Committee on National Security Systems, 26 April 2010. [www.cnss.gov/Assets/pdf/cnssi\\_4009.pdf](http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf)
- [21] Basic concepts and taxonomy of dependable and secure computing, Avizienis, A., Laprie, J.-C., Randell, B., Landwehr, C., Vytutas Magnus Univ., Kaunas, Lithuania. *IEEE Transactions on Dependable and Secure Computing*, Issue Date: Jan.-March 2004 , Volume: 1 Issue:1 , page(s): 11 - 33 , ISSN: 1545-5971.
- [22] J.C. Laprie, Dependability of computer systems: concepts, limits, improvements, in: *Proceedings of the Sixth International Symposium on Software Reliability Engineering (ISSRE’95)*, 1995, pp. 2–11.
- [23] Bishop, Matt, *Computer Security, Art and Science*, published by Addison-Wesley, New York, copyright Pearson Education, Inc., 2003, page 6.
- [24] Jerome Saltzer, Protection and the Control of Information Sharing in Multics, *CACM* 1974, volume 17, issue 7, page 389.
- [25] Jerome Saltzer, Protection and the Control of Information Sharing in Multics, *CACM* 1974, volume 17, issue 7, page 389.

- [26] Basic concepts and taxonomy of dependable and secure computing, Avizienis, A., Laprie, J.-C., Randell, B., Landwehr, C., Vytautas Magnus Univ., Kaunas, Lithuania. IEEE Transactions on Dependable and Secure Computing, Issue Date: Jan.-March 2004 , Volume: 1 Issue:1 , page(s): 11 - 33 , ISSN: 1545-5971.
- [27] Insulin Study Could Lead to New Dosage Devices, NATASHA SINGER, Published: February 4, 2010, New York Times, [http://www.nytimes.com/2010/02/05/business/05diabetes.html?\\_r=1](http://www.nytimes.com/2010/02/05/business/05diabetes.html?_r=1), (Viewed August, 2010).
- [28] Abnormal Heart Rhythms and Pacemakers, Heart Disease Health Center, WebMD, <http://www.webmd.com/heart-disease/abnormal-rhythms-pacemaker>, (viewed, October, 2010).
- [29] International Classification of Diseases, Tenth Revision, Clinical Modification (ICD-10-CM), Classification of Diseases, Functioning, and Disability; copyright World Health Organization (WHO); Center for Disease Control, <http://www.cdc.gov/nchs/icd/icd10cm.htm>. (viewed July, 2010).
- [30] Mortality Data, National Vital Statistics System, Center for Disease Control, <http://www.cdc.gov/nchs/deaths.htm> (viewed July, 2010).
- [31] ICD-10-CM TABULAR LIST of DISEASES and INJURIES, Classification of Diseases, Functioning, and Disability, Centers for Disease Control and Prevention, 1600 Clifton Rd. Atlanta, GA, [ftp://ftp.cdc.gov/pub/Health\\_Statistics/NCHS/Publications/ICD10CM/2010/I10tab2010.zip](ftp://ftp.cdc.gov/pub/Health_Statistics/NCHS/Publications/ICD10CM/2010/I10tab2010.zip) (created 12/23/2009) (downloaded August, 2010).
- [32] “Who Has Rights to a Deceased Patient’s Records?” Aug 04, 2009 08:02 pm | posted by Chris Dimick <http://journal.ahima.org/2009/08/04/rights-to-deceased-patient-records/> Journal of AHIMA.
- [33] Sandhu, R., Coyne, E., Feinstein, H., and Youman, C. 1996. Role-based access control models. IEEE Computer., 29, (2), (Feb).
- [34] Context sensitive access control, Hulsebosch, R J | Salden, A H | Bargh, M S | Ebben, P W G | Reitsma, J, Symposium on Access Control Models and Technologies: Proceedings of the tenth ACM symposium on Access control models and technologies; 01-03 June 2005. Presentation slides online at <http://wwwes.cs.utwente.nl/safe-nl/meetings/18-11-2005/bob.pdf> (viewed October, 2010).
- [35] Atluri, V., Chun, S.A.: A geotemporal role-based authorisation system. International Journal of Information and Computer Security 1(1–2) (2007) 143–168
- [36] A Spatio-temporal Role-Based Access Control Model, Indrakshi Ray and Manachai Toahchoodee, Data and Applications Security XXI, Lecture Notes in Computer Science, 2007, Volume 4602/2007, 211-226, DOI: 10.1007/978-3-540-73538-0\_16 <http://www.springerlink.com/content/c3t50338535hx115> (viewed November, 2010).

- [37] A Fuzzy Role Based Access Control Model for Database Security, U.H.G.R.D Nawarathna and S.R. Kodithuwakku, Proceedings of the International Conference on Information and Automation, December 15-18, 2005, Colombo, Sri Lanka.  
<http://www.ent.mrt.ac.lk/iml/ICIA2005/Papers/SL018CRC.pdf> (viewed November, 2010).
- [38] Ni, Q., Trombetta, A., Bertino, E., Lobo, J.: Privacy aware role based access control. In: SACMAT '07. Proceedings of the 12th ACM symposium on Access control models and technologies. ACM Press, Sophia Antipolis, France (2007).
- [39] Barth, A., Mitchell, J. C., and Rosenstein, J. 2004. Conflict and combination in privacy policy languages. In WPES '04: Proceedings of the 2004 ACM workshop on Privacy in the electronic society. ACM Press, New York, NY, USA, 45–46.
- [40] D. Richard Kuhn, Edward J. Coyne, Timothy R. Weil, "Adding Attributes to Role-Based Access Control," Computer, pp. 79-81, June, 2010 .  
<http://www.computer.org/portal/web/csdl/doi/10.1109/MC.2010.155> and  
<http://csrc.nist.gov/groups/SNS/rbac/documents/kuhn-coyne-weil-10.pdf>
- [41] Overview of Connexx software, Siemens Hearing Instruments, Siemens Audiologische Technik GmbH,  
<http://hearing.siemens.com/en/01-professional/03-partner-solutions/06-connexx/connexx.jsp>  
(viewed November, 2010).
- [42] Email “Inquiry from the SHI Professional website” from Thomas A. Powers, Ph.D., Vice President, Compliance Officer / SOA Officer, Siemens Hearing Instruments, Inc., November 27, 2010.
- [43] “Mobile Medicine, Electrocardiogram-Equipped Cell Phone Allows Remote Monitoring”, Corinne Iozzio, Popular Science, Volume 277, Number 5, October, 2010, page 19. Posted 10.25.2010 <http://www.popsci.com/gadgets/article/2010-10/electrocardiogram-equipped-cell-phone-allows-remote-monitoring> (viewed October 2010). “The Doctor in the Pocket”, H’andy Sana 210, <http://www.handysana.com/>, viewed October 15, 2010.
- [44] ICE: In Case of Emergency, Appventive, LLC., <http://www.appventive.com/ice>  
(application initially downloaded July, 2010; continuously updated).
- [45] CardioTrainer, WorkSmart Labs, Inc., <http://www.worksmartlabs.com/> (viewed October, 2010).
- [46] “About Google Health”, Google, <http://www.google.com/intl/en-US/health/about/> (viewed November, 2010).
- [47] A directory of “Personal health services”, Google Health,  
<https://health.google.com/health/directory?cat=exploremedsandtreatments> (viewed November, 2010).
- [48] Inquiry to developer of ElectricSheep application via email. November 19, 2010.



[49] ElectricSheep developer response via email at address Jon Willis <jondwillis@gmail.com>, November 20, 2010.

[50] “World's Smallest Ultrasound Device Fits In Doc's Coat Pocket”, Rena Marie Pacella, Popular Science, Posted 12.15.2009, <http://www.popsci.com/science/article/2009-12/pocket-sized-scanner-spots-health-troubles#> (viewed November, 2010).

[51] VSCAN jump page, GE Healthcare, a division of General Electric Company, <https://www2.gehealthcare.com/portal/site/vscan2> (viewed November, 2010).

[52] “GE's Vscan puts ultrasound tech in docs' pockets”, by Elizabeth Armstrong Moore, cnet News, posted February 15, 2010, [http://news.cnet.com/8301-27083\\_3-10453496-247.html#ixzz15dNO4EGC](http://news.cnet.com/8301-27083_3-10453496-247.html#ixzz15dNO4EGC) (viewed November, 2010).

[53] Classification of Diseases, Functioning, and Disability. National Center for Health Statistics, CDC. <http://www.cdc.gov/nchs/icd/icd10cm.htm#10update> Retrieved 10/08/2010.

[54] Siemens Hearing Instruments – Troubleshooting, Siemens Audiologische Technik GmbH 1999-2010, <http://hearing.siemens.com/en/04-products/22-explorer/06-use-care/03-troubleshooting/troubleshooting.jsp> (viewed November, 2010).