Remote Home Health Care Technologies: How to Ensure Privacy? Build It In: *Privacy by Design*

November 2009

Information and
Privacy Commissioner,
Ontario, Canada

GE Healthcare

Acknowledgements

The authors wish to acknowledge Ken Anderson, Assistant Commissioner, Privacy, Michelle Chibba and Vance Lockton, Policy Department staff at the Information and Privacy Commissioner's Office, Ontario, Canada, for their input on this paper, as well as Brian Huseman of Intel and Marilyne St. Pierre from GE Healthcare.

Table of Contents

Foreword

Current advances in connectivity, sensor technology, computing power and the development of complex algorithms for processing health-related data are paving the way for the delivery of innovative long-term health care services in the future. Given the demographics of our aging population, there is a critical need for such innovations. Recent technological developments, including medication reminder systems, implanted heart monitors, and other home health care systems, will assist the elderly and infirm to live independently, at home, for much longer periods. Along with these advances come valid privacy and security questions arising from the fact that the data collected and transmitted through these technologies could also include individual monitoring as well as unauthorized access to critical diagnostic and other health data. In the wrong hands, this information could lead to serious personal consequences for those whose data has been compromised, and legal penalties for those responsible.

As the Information and Privacy Commissioner of Ontario, Canada, my mandate is to raise awareness of privacy-related issues involved in emerging technologies or new programs that may impact one's privacy. I am pleased to have partnered with Intel and GE Healthcare to produce this white paper regarding the innovative work being done in the area of applying technologies to home health care. The technology currently available, combined with the continuing research and development in this field, provide a compelling vision of the future possibilities and benefits for home health care.

My message has consistently been that respecting people's privacy should never present an impediment to the delivery of health care services. I call this a 'positive-sum' paradigm – where system functionality and privacy are both delivered in unison – a result that may be achieved by incorporating privacy into the design phase of technologies, namely, by employing *Privacy by Design*. Given the sensitive nature of health-related information, these highly beneficial systems will only succeed if they are built with privacy in mind – thereby delivering a positive-sum, win-win outcome.

I would like to thank my co-authors, David Hoffman, Director of Security Policy and Global Privacy Officer at Intel, and Scott Killen, Global Privacy and Data Protection at GE Healthcare, for their strong contribution to proactively incorporating privacy in their work.

We advance the view that *Privacy by Design* is the sine qua non or the essential element that must be embedded in advances in technology, data management and applications of remote technologies to health care services. We hope to present a strong business case for this in the pages that follow.

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner
Ontario, Canada

I Introduction

Factors such as paper-based systems, aging populations, and increasing rates of chronic disease are overwhelming even the most efficient health care systems. Technology has the potential to move health care to a more proactive, consumer-centric model of care, capable of improving the cost, quality, and accessibility of health care services.

Home-based systems are a particularly promising application of health technology[1]. Many remote home health care systems allow individuals to personalize and customize devices, with the goal of enabling greater patient freedom, reducing costs, and improving the ability for patients to be able to follow the wellness and treatment plans created for them by their medical practitioners. As such, the home is becoming a locus for health care innovation that may, in the future, compete with the hospital. Technology systems that encourage long term care patients (e.g. seniors and those with chronic illnesses) to maintain their physical fitness, nutrition, social activity, and cognitive engagement, so they may function independently in their own homes, for as long as possible, can help to address the social and financial burdens of an aging population.

Technological systems can also reduce the risk of harm by detecting whether patients are properly following their course of treatment, and by providing communication channels between patients and their care givers and loved ones. Informal caregiving networks, such as family and friends, need options available to them to be able to check in on long term care patients and the infirm, both to increase communication and to respond to emergency situations. Professional caregivers also need access to remote, real-time diagnostic data through home-based technologies that help them conduct remote checkups on their patients, and to potentially detect a number of troubling trends. Remote home health care technologies can help to achieve those goals.

The purpose of this paper is to understand these remote home health technologies and their uses, identify the privacy considerations, and provide an approach whereby privacy can be designed directly into these systems in a positive-sum manner, both protecting the personal data of individuals and maintaining the functionality and health benefits of the technology being used.

1 See, for instance:
* Finkelstein, S., Speedie, S., and Potthoff, S. (2006) Home Telehealth Improves Clinical Outcomes at Lower Cost for Home Healthcare. *Telemedicine and Health*, vol. 12, no. 2, pg 128-136.
* Lundell, J. et al. (2006) *Why Elders Forget to Take Their Meds: A Probe Study to Inform a Smart Reminding System.* 4th International Conference on Smart Homes and Health Telematics – ICOST2006, Belfast, Northern Ireland.
* Meyer, M. et al. (2002) Virtually Health: Chronic Disease Management in the Home. *Disease Management*, vol. 5, no. 2.
* Intel Corp. white papers: *The Emergence of Personal Health Systems: Designing Technology for Patients and Clinicians and Addressing the Challenges of Chronic Illness with Personal Health System Technology.* Available from http://www.intel.com/healthcare/telehealth/whitepapers.htm

II Overview of Remote Home Health Care Technologies

Medication Assistance

There are many different types of remote home health care advances, and medication assistance systems offer a good example. Many individuals take a number of different medications each day. Although it is often difficult to take the right pill at the right time, providing guidance to help patients accurately take their medications could save billions of dollars in health care costs, each year.[2]

One such tool is an electronic caddy that centralizes medications in an automatic dispensing machine with audio prompts for when to take various pills. With a stand-alone system, however, individuals may miss or ignore the caddy prompts and the caddy may not offer assistance if someone deviates from the normal medication routine. Instead, a remotely connected medication system could alert caregivers of improper medication use in real time, offering the opportunity to intervene before any serious health damage is done.

A system of intelligent tracking software coupled with technology that detects whether patients are properly following their course of treatment, and a variety of technologies to communicate with the patient, care givers and loved ones, has the potential to prevent serious harm. The medication prompt reminder may be performed through whatever device works best for the individual – whether that be a watch, a phone, or the TV. The nature of the prompt may also be customized for what works best for the individual – a whisper delivered through a hearing aid, a loud reminder through the television, an audio prompt in the voice of a relative, a text reminder on a screen, or a reminder from a computerized persona.

Telehealth

Telehealth, in which medical information is transmitted over the telephone or Internet, is another example of a remote home health care technology that offers promising benefits for both individuals and the health care system[3]. Such applications can be particularly beneficial for patients who are unable to travel, or for those living in rural or underserved urban areas. Telehealth programs integrating information, telecommunications, and physiological monitoring technology can provide cost-effective, convenient alternatives to in-office visits.

2 Lundell, J. et al. (2006) *Why Elders Forget to Take Their Meds: A Probe Study to Inform a Smart Reminding System.* 4th International Conference on Smart Homes and Health Telematics – ICOST2006, Belfast, Northern Ireland.

3 Finkelstein, S., Speedie, S., and Potthoff, S. (2006) Home Telehealth Improves Clinical Outcomes at Lower Cost for Home Healthcare. *Telemedicine and Health*, vol. 12, no. 2, pg 128-136.

Social Connectedness

In studies of seniors with dementia who are living at home, one area in which those seniors and caregivers need assistance is in maintaining social connectedness with their friends and relatives. Maintaining quality social health can lead to improvement in overall health and help to maintain a greater quality of life.[4]

Providing feedback on social health can make seniors and caregivers more proactive in initiating social contact. For example, in the home of a senior, a display may appear next to the primary telephone, showing the picture of the caller. The picture will only be displayed if the person calling is a part of the senior's social network. Some text explaining the relationship of the caller to the senior may also be displayed, if desired (for example, as a memory aid in cases involving dementia). This functionality becomes particularly important when one considers that recent reports suggest that 35 million people worldwide suffer from Alzheimer's or other forms of dementia, a number that will double every 20 years.[5]

Sensor Technologies

Sensor technologies are a further example of a remote home health care application. In the simplest terms, a sensor is an instrument that measures a physical or environmental characteristic or state and either displays the reading, or transmits that reading for display and/or storage elsewhere. Sensors appear in a nearly endless array of applications, some hundreds of years old. They range from simple thermometers, in which a sensor material (mercury or alcohol, usually) expands within a marked glass tube to display a temperature reading, to gym equipment (stationary bikes, etc.) that uses sensors in handles to measure heart rate (and display this data to the user on-screen), to motion sensing security lights, which are activated by optical or auditory changes in the environment. Even vital military tasks, such as sensing the presence of nuclear, chemical or biological agents (and transmitting these results to a satellite), can be automated with sensor technology. The scope of technologies that can be integrated into sensor-based systems – either as the measuring or display/transmission portions of the sensors – is similarly broad and constantly expanding.

A networked system of sensors could span, depending on the application, an individual's body, his or her home, or even extend throughout his or her property, and could measure any number of characteristics. The type, number, and configuration of sensors will vary based on the needs of the individual. Measurements from these sensors would be collected for processing and analysis within the home and potentially at an external location for access by the care provider.

4 Haslam, C. et al. (2008) Maintaining group memberships: Social identity continuity predicts well-being after stroke. *Neuropsychological Rehabilitation*, vol. 18, no. 5-6, pg. 671-691.
5 World Alzheimer's report, http://www.alz.co.uk/research/worldreport/

III Data Transmission and Analysis

There are two primary means of applying the above described technologies to home health care: 1) for purposes of event-based transmission and analysis, or 2) continuous transmission and analysis, which are described below.

Event-Based

An event-based transmission and analysis system is one that records the occurrence of particular, discrete events, throughout the designated care period. This may include the passing of a motion detector, the opening of a pillbox (the medication assistance example, above), or the taking of a blood glucose reading (the sensor example, above). The data recorded may detail the quality of an event (e.g., a blood pressure reading), or the occurrence of the event (e.g., a pill bottle being opened). These systems tend to be highly unobtrusive – allowing the individual to go about his or her daily routine with few or no modifications. The systems may also be able to collect a greater level of information about an individual (as compared to a home care employee), as an individual may neglect to reveal information such as the frequency of trips to the washroom (a change in which can indicate serious health issues). Further, powerful, highly intelligent algorithms will be used to analyze incoming data and identify any 'problems,' as the data itself may or may not reveal anything of significance in its unprocessed form.

Continuous

For some applications, the use of discrete measurements or stationary measuring devices may not be appropriate, or sufficient. Thus, another option for remote home health care technologies lies in the field of continuous transmission and analysis – those devices that record information constantly while in use. These devices may be removable or permanent, but will generally be attached to the user by some means (carried, worn, attached, implanted, etc.). The device may record data, transmit it, or do both. As is the case with certain discrete-event devices, continuous measuring devices may also automatically connect with an individual's PHR or other electronic medical record or database, or require action to be taken by the user to upload data outside of the immediate sensor network. A number of applications of this technology have been developed, ranging in use from monitoring young children for signs of Sudden Infant Death Syndrome (SIDS), to real-time analysis of the vital signs of fire-fighters, to wireless blood pressure monitors for those with heart conditions.

IV Privacy and Remote Home Health Care Technologies

The above described and other remote home health care technology solutions create the potential for great benefits for individuals. However, for many individuals, the home is a foundational area with the highest level of individual privacy. While in some of the above applications no personal health information is involved[6], other health care applications require the collection, use and transmission of personal health data. Therefore, it is important to consider the privacy implications of these technologies, and to design privacy into their development and implementation.

If privacy can be taken into consideration in the development process, there is great potential that these technologies can actually increase the privacy of the individual, by providing them with greater choice and personal control over how their data is managed. Individuals would have the option of receiving care from the privacy of their own home. Further, to the extent that home health care technologies may provide the ability to proactively avoid medical complications that would require intrusive tests and provision of data, there will likely be greater privacy benefits to the use of the technology. Should these privacy benefits be realized along with the health care advantages, then these technologies will serve a clear positive-sum role in health care provision.

To continue this discussion, an understanding of the relationship between home health care applications and privacy must be created; this is addressed below.

Information Privacy Defined

Information privacy is an individual's ability to exercise control over the collection, use, disclosure and retention of his or her personal information, including personal health information. Personal information (also known as personally identifiable information or "PII") is any information, recorded or otherwise, relating to an identifiable individual. Almost any information, if linked to an identifiable individual, can become personal in nature, be it biographical, biological, genealogical, historical, transactional, locational, relational, computational, vocational, or reputational. The definition of personal information is quite broad in scope. The challenges for privacy and data protection are equally broad.

When considering information and communication technologies, it is important to recognize that privacy subsumes a set of protections that extend far greater than security. We call this "SmartPrivacy."[7] Although building strong technological security features into a technology ("*Privacy by Design*") is vital to protecting against data breaches, they are but only one of the means used to achieve information privacy. Equally important is the development of clear information practices, outlining when, how, and the purposes for which health care

6 Consider an exercise machine at a gym which senses the user's heart rate, and displays it on a screen for that user to monitor. Like other measuring tools, the sensor measures and displays a measureable phenomenon – no different than a reading of the current temperature. It is only when the data is recorded, or associated with a particular individual in some way, that privacy questions arise.

7 SmartPrivacy is a term developed in 2009 by the Information and Privacy Commissioner of Ontario. For more information, please see: http://www.privacybydesign.ca/smartprivacy.htm

providers may routinely collect, use, modify, retain or dispose of PII, and the administrative, technical and physical safeguards in place. Developing supporting policies, procedures and an overall accountable culture of privacy ensures that PII will be handled in a privacy-respective manner by an organization and its employees, whether the PII is in electronic or paper form.

What comes before all of this, right at the outset, is ensuring that privacy is embedded earlier into the design of the systems involved. This is *Privacy by Design*.

Privacy by Design

Privacy by Design (PbD) is a concept developed by Dr. Ann Cavoukian, in the mid-nineties. In brief, PbD is a concept that involves embedding privacy into the design specifications of technologies. This process begins by building the principles of Fair Information Practices (FIPs, see Appendix A) into the design, operation and management of information processing technologies and systems, and then elaborates them to the gold standard of becoming the default. While PbD has information technology as its primary area of application, it has since expanded in scope to include two other areas. In total, the three areas of application are: (1) information technology; (2) accountable business practices; and (3) physical design and networked infrastructure. The current era is one of near-exponential growth in the creation, dissemination, use and retention of personally identifiable information. Whether applied at the level of information technology, business practices or systems, it is more critical now than ever to embrace the *Privacy by Design* approach if privacy, as it is currently known, is to survive well into the 21st century.

Rather than following the conventional zero-sum mindset that pits privacy against availability or some other functionality, where privacy may only be attained at the expense of functionality, organizations recognize that a positive-sum model is far more desirable. Such a win-win scenario, whereby privacy and business interests may all be served, can and must be achieved. This positive-sum model may be achieved if privacy safeguards are proactively built into a system, at the outset. By embracing *Privacy by Design*, leading companies have turned their privacy problems into privacy solutions. In a world of increasingly savvy and privacy-aware individuals, an organization's approach to privacy may offer precisely the competitive advantage needed to succeed. Privacy is essential to creating an environment that fosters trusting, long-term relationships with existing customers, while attracting opportunity and facilitating the development of new ones.

V *Privacy by Design* and Fair Information Practices

Privacy by Design asserts that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must become an organization's default mode of operation. Starting by deploying Privacy-Enhancing Technologies (PETs), we now understand that a more substantial approach is required, extending the use of PETs to PETs *Plus* – involving using a positive-sum, not zero-sum paradigm.

Privacy by Design is a mechanism to integrate Fair Information Practices (FIPs) into a product. There are many valuable instantiations of FIPs, including the early HEW Principles, the OECD Guidelines and the European Union 95/46 Data Protection Directive. In 2005, at the 27th International Data Protection Commissioner's Conference, a working group was assembled to develop a reference set of FIPs, described as the "Global Privacy Standard." The final version of this document was accepted at the 28th International Data Protection Commissioners Conference in the United Kingdom. This document captures 10 technology-neutral principles that can be implemented by *Privacy by Design*: consent; accountability; purposes; collection limitation; use, retention and disclosure limitations; accuracy; security; openness; access; and, compliance (See Appendices A and B for a full list of FIPs and the GPS). Of particular note, the GPS builds upon the strengths of existing codes, containing time-honoured privacy principles, but reflects an enhancement by explicitly recognizing the concept of "data minimization" under the "collection limitation" principle.

Perhaps the best known code of fair information practices was developed by the Organization for Economic Co-operation and Development (OECD), called "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data". These guidelines are as follows:

1) **Collection Limitation Principle** – There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge and consent of the data subject.

2) **Data Quality Principle** – Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

3) **Purpose Specification Principle** – The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4) **Use Limitation Principle** – Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with principle 3, above, except: a) with the consent of the data subject, or b) by the authority of law.

5) **Security Safeguards Principle** – Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

6) **Openness Principle** – There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7) **Individual Participation Principle** – An individual should have the right:

   a. To obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him or her;

   b. To have communicated to him or her, data relating to him or her

      i. Within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him or her;

   c. To be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

   d. To challenge data relating to him/her and, if the challenge is successful to have the data erased, rectified, completed or amended.

8) **Accountability Principle** – A data controller should be accountable for complying with measures which give effect to the principles stated above.

We will explore how *Privacy by Design* may be used to integrate these principles – and data minimization in particular – into specific remote home health care technologies.

Privacy by Design Principles

The principles of *Privacy by Design* (PbD) may be applied to all types of personal information, but should be applied with special rigour to sensitive information such as health information. The strength of privacy protection requirements tend to be commensurate with the sensitivity of the data. The objectives of PbD aim to ensure privacy with a maximum control over one's personal information for individuals, and efficient management of that information by organizations such as health care providers. *Privacy by Design* offers a technology-neutral flexible framework which maximizes the ability of technology innovators to apply the FIPs to technology to protect individual privacy, providing an alternative to sole dependence on technology specific mandates that may have difficulty keeping up with the pace of innovation and technology development. Below are the 7 key principles towards achieving these objectives, given in the context of their application to remote home health technologies.

1. *Proactive* not reactive; *Preventative* not remedial

The *Privacy by Design* approach is characterized by the taking of proactive rather than reactive measures. It anticipates and prevents privacy-invasive events, *before* they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it attempts to *prevent* them from occurring. In

short, *Privacy by Design* comes before-the-fact, not afterwards. This proactive approach is fundamental in an environment where the technology is specifically focused on proactively preventing negative health consequences. One example of this proactive privacy design is the furthering of the principle of Individual Participation found in several electronic health records systems, which integrate the ability for individuals to be able to review the data that pertains to them.

2. Privacy as the *default*

Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, his or her privacy still remains intact. No extraneous action is required on the part of the individual to protect his or her privacy when interacting with the system – it is built into the system, *by default*. This goal of remote home health care technologies helps further the Collection Limitation principle by focusing on how the technology can decrease the overall impact to an individual's privacy.

3. Privacy *embedded* into design

Privacy must be embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality. An example of how embedding privacy into design can further FIPs is the increasing practice of using a secure development lifecycle to protect data managed by the device, thereby furthering the Security Safeguards principle.

4. Functionality – Positive-sum, not zero-sum

Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. *Privacy by Design* avoids the pretence of false dichotomies, such as privacy vs. security, or privacy vs. availability, demonstrating that it is possible to have it all.

In the health technology industry, this positive-sum paradigm is increasingly critical. No patient should be forced to encounter a trade-off between functionality and information security or privacy. The key for these individuals, and these technologies, is to be patient-outcome focussed; however, there is a moral imperative not to force a trade-off between privacy and good health in order to achieve these objectives. In particular, ensuring that the positive-sum paradigm is followed will involve furthering the Use Limitation principle. Individuals should be empowered with choices about the data pertaining to themselves – the purposes for which the data is accessed, and by whom it can be accessed.

5. End-to-end lifecycle protection

Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all data are securely

destroyed, in a timely fashion. Thus, *Privacy by Design* ensures cradle to grave, life cycle management of information, end-to-end. Technology features, such as properly executed log data files, allow organizations increased flexibility to implement the Accountability and Data Quality principles.

6. Visibility and transparency

Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike, in furtherance of the Openness, Purpose Specification and Individual Participation principles. Also, in a system that contains health data the ability to verify both protections and to maintain and check audit logs of accesses to data will be crucial to enable user confidence in the system.

A key point to the transparency within these systems is ensuring that the patient in question knows, or at least can know, what data is being collected, how that data is being used, and who can access it. A natural assumption for many will be that the data in question goes to their health care provider, and that they are collecting only 'what is needed.' This understanding may not be sufficient, however. If there are other uses, accesses, or collections of data, these too must be made clear. In many situations the individual's health care provider will be involved in the implementation of the technology and features can be "designed in" to assist the provider in explaining to the patient how the data will be used.

7. Respect for users' privacy

Above all, *Privacy by Design* requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. This applies to all technologies that collect, use, store or manipulate personal data.

VI Practical Application of Privacy by Design: GE's QuietCare and Intel's Health Guide

In order to demonstrate how the principles of *Privacy by Design* can be incorporated into the design of remote home health care technology, the privacy protections incorporated into two sample technologies from this field will be described.

GE's QuietCare

The first example of home-based technology that will be described is QuietCare® from GE Healthcare[8]. The QuietCare system was designed to provide assisted living facilities with notification of change in established behaviour patterns and notifications that a particular event has occurred. In turn, residents are provided with privacy and independence in their daily lives. The system consists of a series of strategically placed motion detectors, which transmit binary activations to a central receiver (also referred to as a base station) in the residence. This data is then transmitted onto a central server, where a profile of the individual's general routine patterns is constructed. This profile data can then be compared against newly received signals, in order to determine: a) potential medical emergencies (a resident prone to sleepwalking leaves his/her bed and is then detected leaving the residence in the middle of the night), or b) potentially significant changes in routine (frequent / longer trips to the washroom, sleep pattern changes, etc.). Upon detection of an unusual event – such as a change in behaviour that might be indicative of an emerging medical condition – a series of escalating alerts are sent to pre-selected individuals, potentially including the individual him/herself, the individual's family, the caregiver, or emergency services. The number and location of these sensors along with the generated alerts is completely customizable based on the individual's condition and comfort with sensors.

GE's QuietCare system offers a great example of how the principles of *Privacy by Design* can be incorporated into the design of technology. The importance of protecting the privacy of individual health information was not lost on the developers of the system, and in fact, informed certain design choices. As a result, a number of privacy features were built into the QuietCare system, including:

- **Privacy is the default – and the only – setting.** Installers and users of the GE QuietCare system are not in a position to put personal data at additional risk based on configuration or use. The privacy features are fully integrated into the system, and cannot be removed or deactivated by the user. This privacy protection mainly comes from a restricted configuration that does not allow for the entry of non-essential information or the exporting of data to non-target entities.

- **Privacy is embedded into the design.** QuietCare is designed so that sensitive information is not transmitted wirelessly; the only wireless communications are from the sensors to the base station, and these communications are short-range, in a proprietary

8 See http://www.gehealthcare.com/usen/telehealth/quietcare/proactive_eldercare_technology.html. QuietCare is a licensed trademark name of Living Independently Group, LLC

format, and contain only sensor unit ID data. In itself, a sensor ID does not contain any personally identifiable information. Transmissions between the base station and the data server occur only in one direction via the phone line, so the system does not respond to non-authorized queries.

- **Positive-sum functionality.** Part of the most valuable functionality of the QuietCare system comes from the real-time detection of events and availability of information to the caregivers. The design of QuietCare allows the advantages of that functionality while maintaining privacy as well, a *positive-sum* solution. Embedded privacy, as described previously, does not negatively impact the availability of critical information to the caregivers including both real-time alerts and aggregated behavioural trends.
- **Respect for users' privacy.** Access to the reports generated by the QuietCare system occurs through a password-protected and encrypted online interface and access to individual information is restricted to the individual's caregivers. In addition, all access and modifications to an individual's profiles, including edits to such information, are logged and may be audited. This interface also allows the configuration of real-time alerts to be forwarded only to the selected destinations.
- **End-to-end lifecycle protection.** GE's QuietCare example repository and interface is hosted on a central server in a secured and monitored data center. This hosted model provides a number of data protection advantages including rapid response and tightly controlled support personnel. As with any technical data storage solution, the system must be closely monitored and updated with current technology, and such maintenance can occur very rapidly in a central data center with a select group of personnel.

The QuietCare example also highlights the importance of extending the principles of *Privacy by Design* beyond technologies alone, to encompass accountable business practices not only by the vendors, but also by the users. Wireless sensor networks, such as QuietCare, do not *deliver* health care services; instead, they are a tool, designed to monitor activities in order to assist and alert assisted living facilities, who provide the actual care. Thus, data cannot be restricted exclusively to the technological components of the system; at some point, the care provider must gain access to a subset of the relevant information (at a minimum).

The responsibility for determining access rights to a particular individual's information belongs to the care provider in consultation with the individual. Although a vendor may restrict access to stored data through technical access control mechanisms, it is not feasible for a vendor – such as GE Healthcare, in the case of QuietCare – to manage individual accounts. The care provider owns the authorization process of granting access to its individuals' stored data to appropriate personnel. Similarly, the technology vendor is not in a position to provide appropriate notice and consent options to individuals; this is again the responsibility of the care provider that operates the sensor network.

GE's QuietCare system is a great example of how home-based wireless technologies can offer assisted living facilities a passive sensor option while protecting individual privacy, with control over the access to, and the use of, personal information.

Intel® Health Guide

Another home health technology that is currently in the marketplace offers an excellent case study for the *Privacy by Design* framework. The Intel Health Guide[9] is a remote patient monitoring system that combines an in-home patient device with an online interface that allows clinicians to remotely manage care.

From the health care provider perspective, remote home health care technologies can reduce hospitalization and readmission rates by allowing clinical staff to identify changes in patients' health before conditions become acute, to increase patient compliance with disease management programs, and to offer cost-effective extended care to more patients by allowing clinicians to assist patients without in-person visits. They also provide health care organizations with an additional tool to cope with the challenges of chronic care and to increase efficiency. From the patient perspective, remote health care tools allow patients to become more engaged and proactive in their cases and provide health care providers with more informed and personalized information.

The Intel Health Guide offers several features that provide many of the benefits available from remote home health care technologies. First, it offers interactive patient health sessions that are designed and scheduled by the patient's health care professional. During these sessions, the patient can measure their vital signs, respond to health assessment questions, receive educational information and motivational messages, and complete surveys—information that can then be made available to authorized health care professionals to help assess the patient's health status. Second, it offers a multimedia educational library that provides a variety of content, including text, audio, and video, as part of a patient's scheduled health session or offered at a "teachable moment" in the patient's care. Third, the Intel Health Guide offers two-way video calls. An integrated video camera allows health care professionals to arrange and conduct two-way video calls with their patients, helping them strengthen their interaction with their patients by observing them perform specific tasks, or by providing advice and encouragement. Fourth, the Health Guide is provided with validated vital sign devices that can take patient vital sign measurements. Numerous wired and wireless vital sign devices in the market have been tested and validated to ensure interoperability. From blood pressure monitors and glucose meters to pulse oximeters, peak flow meters, and weight scales, measurements can be obtained as part of a regular session scheduled by the clinician or on an ad hoc basis. Finally, the Intel Health Guide provides audio and visual notifications and reminders. With this feature, patients are notified of scheduled sessions with an audible tone and with visual cues that include on screen reminders and a flashing light.

The Intel Health Guide has incorporated a substantial number of privacy protections into the technology itself, providing security and control for both the patient and health care provider. Privacy protections begin with patient consent to use the device. Unlike other consumer products, where the individual alone decides whether to purchase the product and use it in accordance with a company's privacy practices, use of the Intel Health Guide is governed by the doctor/patient relationship. A patient cannot purchase an Intel Health Guide on his or her own. Instead, a physician must prescribe or otherwise provide the

9 See http://www.intel.com/healthcare/ps/healthguide/index.htm

patient with the device and service to monitor certain parameters at home and the patient consents to that use based upon the doctor's advice and their relationship.

Security is designed into the Health Guide. A patient must enter a four-digit personal identification number (PIN) before he or she can use the device. Although a stronger password could have been mandated for the Health Guide, Intel engineers concluded that because the device is not intended for mobile use and because it is located in a patient's residence, then a PIN, coupled with the physical security of the patient home protecting the device itself, was a sufficient amount of security. The Health Guide also contains standard security protections; for example, inactivity requires re-entry of the PIN. It is worth noting that if a patient cannot enter the PIN because the patient is vision- or memory-impaired, then the health care provider can disable the PIN system and document that the patient and provider have agreed upon this opt-out mechanism. Moreover, the hard drive of the Health Guide is encrypted.

Disclosure limitations are also built into the transmission mechanisms of the Health Guide. When a patient receives a device, a professional installer does the configuration. Part of the installation procedure is to ensure that the device is registered to connect with the correct server on the back-end. Thus, even though the data is transmitted over the Internet, the Health Guide is configured to register and communicate only with that patient's health care provider. All data is also encrypted via 128 bit Secure Sockets Layer (SSL/TLS) technology, and the videoconferences between patients and health care providers use VPN technology.

The Health Guide was designed to ensure that only a patient's own health care provider views their personal health information. This "need to know" configuration is an important privacy component, especially because of the particularly sensitive nature of health information. As mentioned, health care providers are able to access their patients' health data that is communicated from the Health Guide by using an online interface. Each health care provider, be it a nurse or a doctor, must have their own credential before accessing the online portal. The online portal has stronger privacy and security protections than the Health Guide, which is necessary because the information is accessible online and in places outside the home. For instance, the online interface requires a strong password and there is a time out for inactivity.

Continuing the "need-to-know" device architecture, Intel has designed the system with restricted access to all PHI. Support personnel can back up data, restore data, and manage the system without access to any sensitive patient data (PHI or PII).

If either a doctor or patient decides to discontinue use of the Intel Health Guide, there are strict procedures in place for deletion of the data. All data is scrubbed off of the device itself and is written over multiple times to ensure that it is not recoverable. Also, at the health care provider's direction, data is also deleted off of Intel servers.

The Intel Health Guide is another prime example of the how companies can use *Privacy by Design* to provide technology that can greatly assist individuals, while at the same time, strongly protecting their privacy.

VII Final Thoughts about Privacy and Remote Home Health Care Technologies

Home health care is not reserved for the elderly. This technology may also be applied to any individual with a chronic condition that requires frequent, or constant, care. However, given the demographics of the aging populations in Canada, the United States and all around the world, along with estimates that only 15 percent of people over 80 *do not* have a chronic condition[10], or that 85 percent of those over 80 *do* have a chronic condition, it becomes clear that remote home health care technologies are poised to become a vital part of the overall health care provision environment.

Individuals who must care for family members with chronic conditions face significant strain, both financially and emotionally. The economic burden to health care systems in these scenarios is also very high. Chronic illness is, of course, most challenging for patients themselves, as they often have to make significant changes to their social and family relationships while dealing with ongoing pain, prolonged medical treatment, and growing restrictions to their daily activities. The psychological impact of allowing caregivers near-constant access to one's life by necessity, can be quite stressful. Elderly or infirm individuals have always wanted the option of maintaining independence, without an associated foregoing of any necessary care. Fortunately, home health care technologies are now starting to allow for this possibility by delivering a growing number of options.

The gains in privacy, independence and quality of care associated with remote home health care technologies cannot be tempered by associated losses in data privacy. The sharing of sensitive health information outside of one's circle of care may cause great distress to patients. Numerous jurisdictions around the world well recognize this fact, and enforce the protection of personal health information through legislative means. However, we must ensure that patient care is not compromised by these protections – privacy should not impede the delivery of health care services. A home health care system would be of little use if valuable information were left inaccessible at times of need. Therefore, we must strive for a positive-sum outcome, in which all interests may gain together.

Using the principles of *Privacy by Design*, the interests of both patient and caregiver may be met, and the provision of home health care may be delivered in a highly effective, privacy-protective manner. Companies such as Intel and GE Healthcare are proving that a positive-sum paradigm is not only desirable – it is indeed achievable – positive-sum, all the way. In home health care, it may be the only way.

10 Intel Health (2007) *Chronic Care at the Crossroads*. Available at: http://www.intel.com/healthcare/Chronic_Care_%A0at_Crossroads_White_Paper.pdf

APPENDIX A: Fair Information Practices

(Source: CSA International's *Model Code for the Protection of Personal Information*)

1. **Accountability:** An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

2. **Identifying Purposes:** The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

3. **Consent:** The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate.

4. **Limiting Collection:** The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

5. **Limiting Use, Disclosure and Retention:** Personal information shall not be used or disclosed for purposes other than those for which it is collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of the stated purposes.

6. **Accuracy:** Personal information shall be as accurate, complete and up to date is necessary for the purpose for which it is used.

7. **Safeguards:** Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8. **Openness:** An organization shall make specific information about its policies and practices relating to the management of personal information readily available to individuals.

9. **Individual Access:** Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information, and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended, as appropriate.

10. **Challenging Compliance:** An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

APPENDIX B: Global Privacy Standard

Creation of a Global Privacy Standard

By Commissioner Ann Cavoukian, Ph.D.

Introduction

In 2005, at the 27th International Data Protection Commissioners Conference in Montreux, Switzerland, I chaired a Working Group of Commissioners. This Working Group was convened for the sole purpose of creating a single Global Privacy Standard. Faced with globalization and convergence of business practices, regardless of borders, I thought there was a pressing need to harmonize various sets of fair information practices into one Global Privacy Standard. Once such a foundational policy piece was in place, then businesses and technology companies could turn to a single instrument for evaluating whether their practices or systems were actually privacy enhancing, in nature and substance.

While attempting to develop a single law on data protection was beyond our reach, I was confident that we could develop a single privacy instrument, globally. In advancing my objective to develop a harmonized set of fair information practices, my office embarked on the preliminary work of conducting a "Gap Analysis." This was the process of comparing leading privacy practices and codes from around the world, comparing their various attributes, and the scope of the privacy principles enumerated therein. We identified the strengths and weaknesses of the major codes in existence and then tabled our Gap Analysis with the Working Group of Commissioners.

In the months that ensued, we embarked upon the work of harmonizing the principles into a single set of fair information practices. This led to the development of the attached Global Privacy Standard (GPS), which builds upon the strengths of existing codes containing time-honoured privacy principles and, for the first time, reflects a noteworthy enhancement by explicitly recognizing the concept of "data minimization" under the "collection limitation" principle.

After successive drafts of the GPS were developed, revised and circulated for review, the attached final version of the GPS was formally tabled and accepted in the United Kingdom, on November 3, 2006, at the 28th International Data Protection Commissioners Conference.

Objective

The objective of the Global Privacy Standard is to form a set of universal privacy principles, harmonizing those found in various sets of fair information practices presently in existence.

The Global Privacy Standard draws upon the collective knowledge and practical wisdom of the international data protection community.

Scope

The Global Privacy Standard reinforces the mandate of privacy and data protection authorities by:

- focusing attention on fundamental and universal privacy concepts;
- widening current privacy awareness and understanding;
- stimulating public discussion of the effects of new information and communication technologies, systems, standards, social norms, and laws, on privacy; and
- encouraging ways to mitigate threats to privacy.

The GPS informs developers and users of new technologies and systems that manage or process information. The GPS may be particularly useful when developing information and communication technology standards, specifications, protocols, and associated conformity assessment practices.

The GPS can assist public policymakers when considering laws, regulations, programs and the use of technologies that may impact privacy. The GPS can equally assist businesses and developers of technology that may have an impact on privacy and personal information.

The GPS addresses privacy concerns for decision-makers in any organization that has an impact on the way in which personal information is collected, used, retained, and disclosed.

The GPS is not intended to pre-empt or contradict any other laws or legal requirements bearing upon privacy and personal information in various jurisdictions.

GPS Privacy Principles

1. **Consent:** The individual's free and specific consent is required for the collection, use or disclosure of personal information, except where otherwise permitted by law. The greater the sensitivity of the data, the clearer and more specific the quality of the consent required. Consent may be withdrawn at a later date.
2. **Accountability:** Collection of personal information entails a duty of care for its protection. Responsibility for all privacy related policies and procedures shall be documented and communicated as appropriate, and assigned to a specified individual within the organization. When transferring personal information to third parties, organizations shall seek equivalent privacy protection through contractual or other means.
3. **Purposes:** An organization shall specify the purposes for which personal information is collected, used, retained and disclosed, and communicate these purposes to the individual at or before the time the information is collected. Specified purposes should be clear, limited and relevant to the circumstances.

4. **Collection Limitation:** The collection of personal information must be fair, lawful and limited to that which is necessary for the specified purposes.

   Data Minimization – The collection of personal information should be kept to a strict minimum. The design of programs, information technologies, and systems should begin with non-identifiable interactions and transactions as the default. Wherever possible, identifiability, observability, and linkability of personal information should be minimized.

5. **Use, Retention, and Disclosure Limitation:** Organizations shall limit the use, retention, and disclosure of personal information to the relevant purposes identified to the individual, except where otherwise required by law. Personal information shall be retained only as long as necessary to fulfill the stated purposes, and then securely destroyed.

6. **Accuracy:** Organizations shall ensure that personal information is as accurate, complete, and up to date as is necessary to fulfill the specified purposes.

7. **Security:** Organizations must assume responsibility for the security of personal information throughout its life cycle consistent with the international standards that have been developed by recognized standards development organizations. Personal information shall be protected by reasonable safeguards, appropriate to the sensitivity of the information (including physical, technical and administrative means).

8. **Openness:** Openness and transparency are key to accountability. Information about the policies and practices relating to the management of personal information shall be made readily available to individuals.

9. **Access:** Individuals shall be provided access to their personal information and informed of its uses and disclosures. Individuals shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. **Compliance:** Organizations must establish complaint and redress mechanisms, and communicate information about them to the public, including how to access the next level of appeal. Organizations shall take the necessary steps to monitor, evaluate, and verify compliance with their privacy policies and procedures.

About the Authors

Ann Cavoukian, Ph.D., Information and Privacy Commissioner of Ontario, Canada

Dr. Ann Cavoukian is recognized as one of the leading privacy experts in the world. Noted for her seminal work on Privacy Enhancing Technologies (PETs) in 1995, her concept of *Privacy by Design* seeks to embed privacy into the design specifications of technology, thereby achieving the strongest protection. An avowed believer in the role that technology can play in protecting privacy, Dr. Cavoukian's leadership has seen her office develop a number of tools and procedures to ensure that privacy is strongly protected, not only in Canada, but around the world. She has been involved in a number of international committees focused on privacy, security, technology and business, and endeavours to focus on strengthening trust and confidence in emerging technological applications. Dr. Cavoukian also serves as the Chair of the Identity, Privacy and Security Institute at the University of Toronto, Canada. Recently reappointed as Commissioner for an unprecedented third term, Dr. Cavoukian intends to grow *Privacy by Design* and hopes to make it go "viral."

David A. Hoffman, Director of Security Policy and Global Privacy Officer, Intel Corporation

David A. Hoffman is Director of Security Policy and Global Privacy Officer at Intel Corporation, in which capacity he heads the organization that oversees Intel's privacy compliance activities, legal support for privacy and security and all external privacy and security engagements. Mr. Hoffman joined Intel in 1998 and in 1999, he founded Intel's Privacy Team. In 2008, the European Commission selected Mr. Hoffman as one of five members of its Data Protection Expert Group. Mr. Hoffman served on the TRUSTe Board of Directors from 2000-2006, where he was Chair of the Compliance Committee of the Board. Also, in 2005 Mr. Hoffman was appointed to the Department of Homeland Security's Data Privacy and Integrity Advisory Committee, on which he is Chair of the Data Sharing and Use Subcommittee. Mr. Hoffman is also on the Board of Directors for the International Association of Privacy Professionals, on which he is the Board's Treasurer. Mr. Hoffman holds the Certified Information Privacy Professional Certification. Mr. Hoffman has lectured at law schools in the US, Europe and China. Mr. Hoffman has a JD from The Duke University School of Law, where he was an Editor on the Duke Law Review. Mr. Hoffman also received an AB from Hamilton College.

Scott Killen, Manager for Global Privacy and Data Protection, GE Healthcare

Scott Killen is the Manager of Privacy and Data Protection globally for GE Healthcare Systems. His role includes the responsibility of privacy and security compliance for GE's operations in the healthcare environment as well as representing GE Healthcare to the industry on data protection matters. Mr. Killen has worked in the healthcare technology space for 10 years in several privacy and security capacities, such as product development, audit lead, risk manager, and legal. He also holds multiple professional certifications related to data protection including Certified Information Privacy Professional and Certified Information System Security Professional. Mr. Killen received his Bachelors of Science degree from Purdue University and Masters in Business from Marquette University.

Information and Privacy Commissioner of Ontario, Canada
2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8
Website: www.ipc.on.ca
Privacy by Design: www.privacybydesign.ca
Telephone: 416-326-3333
Fax: 416-325-9195

Intel®
2200 Mission College Blvd.
Santa Clara, CA 95054-1549
U.S.A.
Telephone: 408-765-8080
Website: www.intel.com

GE Healthcare
3000 North Grandview
Waukesha, WI 53188
U.S.A.
Telephone: 1-800-526-3593
Fax: 1-877-295-8102
Website: www.gehealthcare.com

The information contained herein is subject to change without notice. Intel®, GE Healthcare, and IPC shall not be liable for technical or editorial errors or omissions contained herein.

November 2009

intel

Information and Privacy Commissioner, Ontario, Canada

GE Healthcare