Preface

The cost of care today has created incentives for many of the stakeholders within the healthcare industry and government health agencies to devote time and resources towards acceleration of technology adoption to help manage those costs. While individual countries approach how to integrate technology into their own particular healthcare system depending on their own cultures and experience, this book demonstrates that regardless, they are all increasingly reliant on the use of technology to create efficiencies in those systems.

The first section of this book is designed to elaborate on some of the new trends within health technologies. The healthcare industry has long operated using paper records along with a combination of silo-based clinical specialization systems. There is a significant push going on in the United States, Europe and in other developing countries. The United Kingdom, in particular, has been one of the leaders of leading technology trends within the healthcare industry.

The first chapter speaks to one of the most comprehensive and far reaching healthcare technology efforts that are currently under way in the United States. This project is an extension of previous efforts by the federal government to accelerate the use of Electronic Health Records (EHR). There has been sufficient progress made towards this adoption that the legislative efforts have shifted focus to the potential uses of this electronic data that is being collected and stored via EHRs. One of the primary uses facilitated through the most recent legislation directed at economic stimulus and health reform includes the creation of the technical, procedural, semantic framework that is necessary to engage in widespread, large scale medical research projects. These medical research projects are expected to identify superior therapies and medications which will be applied to best practice. The assumption is that through creation of a National Health Information Network (NHIN) to allow for easy exchange of large amounts of health data these best practices can be identified and integrated into the system in such a way as to reduce the cost of healthcare delivery. This form of research is known as Comparative Effectiveness Research (CER). One of the biggest potential barriers to the success of the NHIN and CER is the perception that this will result in rationing of healthcare. The proponents of the NHIN and CER are pouring substantial financial incentives into the system to advance their usage, while the opponents of the NHIN and CER are pledging to ‘repeal and replace’ much of what has been proposed.

The 2nd chapter in the book identifies the impact of technology adoption on the privacy rights of disabled individuals. The author makes a case for the fact that disabled individuals have the potential to be more directly impacted by potential privacy threats of electronic health data. This increase in the potential risk relates to the fact that the disabled are more likely to have private medical issues that could present barriers in insurance and employment. The disabled population is also more likely to be more often seen by more individual providers than their able bodied peers. These more frequent interactions
with the healthcare system that generates more sensitive health information puts this population at higher risk of having the information compromised.

The move towards electronic health data collection and storage has motivated stakeholders within the healthcare industry to explore technical controls to assist with the protection of this data. The Hippocratic Database and Active Enforcement are examples of technologies being proposed to accomplish this goal through granular access and audit controls built in to clinical systems. The author outlines how these technologies can be used to support protection of health data and makes a case for how it can also be helpful in meeting more stringent health protection laws that impact the global use and exchange of health data.

The National Health Information Network (NHIN) is one of the most ambitious proposals of how technology can be used to support the healthcare industry among a number of proposals. The preliminary efforts towards creation of the NHIN involve several federal agencies and a small handful of private providers. The intent is to leverage the Internet as the backbone for this network and the existing pilot is intended to prove the viability of this approach. The author identifies a range of potential barriers and challenges that have the potential to impede or prevent these plans from coming to fruition.

One of the objectives behind the promotion of accelerated adoption of technology by governments all over the developed world is the need or desire to reduce the cost of administering healthcare. This author identifies one approach being used in the UK that will reduce the cost of maintaining patient demographic and activity information by providing a kiosk approach that allows patients to do their own data entry into these systems. The various kiosk solutions that are available to fill this role are explored and the benefits and challenges of their use are explored, as well.

The final chapter in this section of the book consists of a study that looks at the readiness of the Scottish health system to leverage the principles and benefits of eHealth solutions. The study is a follow-up of a previous study and is meant to confirm or deny the results of that previous study.

The second section of the book involves a look at the security solutions that are being implemented in the healthcare industry in response to the adoption of changing trends and new technologies.

The move towards electronic health records has created a new and more urgent need for healthcare providers to have and maintain an aggressive and comprehensive disaster recovery and business continuity program. Failure to invest time and resources in hardware, software and data redundancy can be a fatal mistake for healthcare providers who will no longer have a paper record to use as backup. This author explores the important components that are critical to an effective disaster recovery and business continuity plan for those organizations that have made the move to electronic health data collection and storage.

Those information security professionals that work in the finance industry have long been aware of the potential for risks pertaining to discovery of electronic data as part of a criminal or civil lawsuit. As the healthcare industry moves towards electronic data collection and storage the potential for the industry to face some of these same risks increases as well. This author explores some of those unexpected outcomes and offers advice as to how healthcare organizations might mitigate some of those risks.

The healthcare industry has been identified by criminals as high potential for engaging in identify theft. The industry has long collected and used social security numbers as a means to differentiate patients and as a part of their payment process. Much of the risk and activity involving identify theft involves trusted insiders making this particular problem particularly tough for the industry to manage. This author explores the role that biometric controls might play in mitigation of the risk of identity theft by associating this biometric with a transaction.
A large challenge facing those who are working towards widespread, large scale health research projects is having the tools necessary to evaluate the trustworthiness of this data that is coming from a large number of different providers. There are a range of factors that contribute to trustworthiness including accuracy, validity, rigor in collection processes, integrity controls etc. This author considers the factors that contribute to trustworthiness of health data and proposes a model that researchers or others who are interested in secondary use of health data can apply to mitigate some of the risks of using data from multiple sources.

There is a trend in the information security industry towards implementation of two factor authentication as a replacement for reliance on simple passwords to protect data. Implementation of two factor authentication is just beginning to be seen in the healthcare industry. The final chapter in this section of the book takes another look at the use of biometric technologies as a means of controlling access to healthcare data. The author explores some of the potential benefits and challenges to using this technology.

The third section of this book focuses on some of the really tough ethical issues that are being created as a byproduct of technology adoption within the healthcare industry. Information security and other healthcare professionals face hard choices every day as to how to properly balance security controls with data availability and access.

One of the tools that are being used in a variety of ways within the healthcare industry is Radio Frequency Identification or RFID technology. This technology has been adopted as a more sophisticated replacement for older bar coding technology as a means of tracking inventory and supply chain management. These kinds of implementations that relate to tracking of inanimate objects are not seen as highly controversial. The ethical aspects of how this technology is being used relate to when it is applied to tracking or otherwise monitoring the location or activities of human beings. The author describes how this technology is being used and what some of the ethical issues are in how it is being used. Examples include tracking of patients, as well as staff, and some evidence of potential health concerns that may relate to the use of this technology that might be considered by organizations seeking to leverage the benefits of RFID technologies.

As the healthcare industry moves towards electronic collection and storage of health data there will be an increased movement towards associating this data with the Internet. This author explores the privacy implications around collection and exchange of sensitive health data and the ability, or inability, of providers to secure this information and the potential that providers currently underestimate the level of risk to privacy and overestimate their ability to protect the information from unauthorized disclosure as a consequence of associating it with the Internet.

Nurses are among those within the healthcare industry who are most impacted by technology adoption and ethical issues. This author explores ethical issues facing the nursing profession including those related to global education and migration and how technology might address nursing shortages in different parts of the world.

The final chapter of this book is an ethical opinion paper that looks at how the healthcare industry is leveraging technology or, failing to leverage technology for optimal return on investment. The industry that began in a highly segmented and locally controlled data collection and storage environment is now moving toward a more integrated environment. The author looks at how the industry might be more effective in how technology is integrated into the overall work processes to maximize the benefit that this technology adoption can provide to the industry.
The authors of the chapters within this book have documented examples for how their particular country or aspect of the healthcare system are integrating healthcare technology and how that technology may impact the security, privacy and medical ethics of patients and practitioners. The information in these chapters offers useful insights for those charged with leveraging technology to enhance and improve the healthcare system in other countries.