Chapter 9
Ethics, Privacy, and the Future of Genetic Information in Healthcare Information Assurance and Security

John A. Springer
Purdue University, USA

Jonathan Beever
Purdue University, USA

Nicolae Morar
Purdue University, USA

Jon E. Sprague
Ohio Northern University, USA

Michael D. Kane
Purdue University, USA

ABSTRACT

The risks associated with the misuse and abuse of genetic information are high, as the exploitation of an individual's genetic information represents the ultimate example of identity theft. Hence, as the frontline of defense, information assurance and security (IAS) practitioners must be intimately familiar with the multidimensional aspects surrounding the use of genetic information in healthcare. To achieve that aim, this chapter addresses the ethical, privacy, economic, and legal aspects of the future uses of genetic information in healthcare and discusses the impact of these uses on IAS. The reader gains an effective ethical framework in which to understand and evaluate the competing demands placed upon the IAS practitioners by the transformative utility of genomics.

DOI: 10.4018/978-1-61692-245-0.ch009

INTRODUCTION

Biotechnology and its related applications are advancing rapidly. As readers in the field of information assurance and security, you may wonder what biotechnology advancements have to do with information security. The intersection is clearly seen when one considers the fact that the human genome is made up of over 3 billion bits of *information*, where these bits are nucleotide base pairs. Viewed in this context, the human genome as information is slightly different in nature from other forms of personal information, such as a social security number, a credit card number, your name, your address, and so on. The difference is as follows. If an individual's social security or credit card number is compromised, she can get a new one – albeit not without some effort and cost. In fact, one can even get a new name. This is not the case with your genome. In this case, you are your information and always will be. Furthermore, the utility of this information could extend beyond your life. Your children and grandchildren are derived from your genome; they are information derivatives.

As such, consideration of the use and potential misuse of genetic information seems highly relevant to information assurance and security. We believe that IAS practitioners should be aware of the evolution of biotechnology and the consequent implications for the use of genetic information. Toward this end, this chapter discusses a particular area, known as pharmacogenomics, which is overviewed in the next section, and considers some of the ethical, privacy, economic, and legal aspects of the future uses of genetic and pharmacogenomic information in healthcare.

We begin with an overview of pharmacogenomics so that readers have a basic grounding. Next this chapter discusses the promise of technological innovation so that readers understand how advances are perceived as beneficial to society. Then we analyze ethics and genetic information, with a concentrated focus on ethics and pharmacogenomics. The analysis serves as a model demonstrating how critical ethical analysis of past innovations can serve to reveal whether or not there really is anything "ethically new" here. As you'll see, we conclude that with regard to pharmacogenomics, yes, there are a few novel challenges for consideration. Given that many ethical challenges are linked to public policy and social norms, we turn to discussion of how existing laws and social norms may or may not address/influence some of these challenges. Finally, we end by discussing implications for models of information assurance and security, bringing full circle the ramifications of biotechnology to information assurance and security.

Before we proceed to a discussion of background topics, let us highlight relevant information assurance and security concepts as these are some of the criteria by which we later evaluate the pertinent ethical issues that arise from the use of genetic information in healthcare. According to Bishop (2002) as well as Whitman and Mattord (2005), the fundamental IAS concepts include confidentiality (which includes privacy), integrity, availability, and evidence of trustworthiness. Confidentiality is the concealment of information or resources, and access control mechanisms help to enable confidentiality (Bishop, 2002); generally speaking, confidentiality has a close relationship with privacy (Whitman & Mattord, 2005). Privacy is a complex concept with many nuanced definitions (Schoeman, 1984); for our purposes, we delimit the definition of privacy to one's independent control over the public dissemination of one's personal information. Integrity, according to Bishop, refers to the trustworthiness of data or resources, and is usually operationalized in terms of preventing improper or unauthorized change. As such, integrity entails mechanisms that prevent modification or detection of the integrity of the data (Bishop, 2002). In tandem with confidentiality and integrity comes availability, which concerns access to the desired information or resources (Bishop, 2002); a classic example of not providing avail-