Bioelectronic Medicine

# Melissa Masters's Response to "Imagining the Future of Medicine" Commentary

*Melissa Masters*

Battelle Memorial Institute, Columbus, Ohio, United States of America

Ms. Masters is Director of Electrical, Software and Systems Engineering at Battelle and heads Battelle's DeviceSecure Services. Ms. Masters has more than 15 years of experience in product development as a project manager, systems engineer and design engineer, serving as the project manager and lead systems engineer on medical device development and sustaining engineering programs. Ms. Masters is a voting member of the Association for the Advancement of Medical Instrumentation (AAMI) working group on cybersecurity for medical devices and contributed to the vulnerability model for AAMI's TIR 57. She has given conference presentations, been published and widely quoted on a variety of medical cybersecurity topics in AAMI Horizons, Mass Device, ExecutiveGov.com, and Fierce Medical Devices. In addition, Ms. Masters holds a Regulatory Affairs Certification (RAC) and has a working knowledge of domestic and international regulatory requirements for medical devices.

**Online address: www.bioelecmed.org**
**doi: 10.15424/bioelectronmed.2015.00009**

Everyone wants to prevent illness before it starts. Everyone wants more time and energy for the activities they enjoy most. In other words, everyone wants to be healthy and feel good all the time, automatically. The vision laid out in Imagining the Future of Medicine could enable just that. But underpinning this compelling vision is ubiquitous connectivity where every connection, every interface, and every transmission of data represents a security challenge.

In Imagining the Future of Medicine, life-affecting decisions regarding a person's health will be made automatically on the basis of collected information. Any alteration of data, intentional or not, could put that person's life at risk through the resulting decisions that are executed. Therefore, upholding the C.I.A. (confidentiality, integrity and availability) of data security within this envisioned ecosystem is critical.

Imagine this scenario: Sam's glucose monitor and his insulin pump are connected. This closed loop system takes readings and provides insulin dosing based on those readings. Sam has an artificial pancreas, the "holy grail" of diabetes management. While the device monitors Sam's physiology, it is itself being monitored externally by Sam's doctors. Collected information is uploaded automatically into Sam's electronic health record (EHR). When Sam's supply of insulin is low, a prescription is automatically ordered and shipped. Such benign and passive monitoring unintentionally provides an electronic gateway into Sam's artificial pancreas. Imagine that connection is exploited by a "black hat" hacker, who alters the data to indicate that Sam's glucose level is hyperglycemic. Sam's device compensates and delivers a dose of insulin far greater than it should be, causing a potentially fatal hypoglycemic episode.

This level of system integration will be obtainable in the near future. And while the scenario seems implausible, it will be possible.

More immediate is the threat of confidentiality breach in health records. Disturbingly, numerous incidents have been reported in the past two years, shaking the public's faith in the security of our health care system. It's not hard to imagine scenarios in which a person's health data could be held hostage, with a demand to pay ransom or risk having the health information go public. Health identities could also be stolen outright and used to commit insurance or other fraud similar to credit card crimes. It's fairly simple to get a new credit card number, but a person only has one identity, and if it is stolen it is much more difficult to recover. Too many incidents like this could turn public sentiment to fear and distrust, hindering the adoption of an integrated, connected system for our records and data.

So what can be done to reap the powerful benefits envisioned in Imagining the Future of Medicine? An important first step is to mindfully identify, analyze, mitigate and control the risks to the

***Address correspondence to*** *the Journal: editor@bioelecmed.org.*
*Submitted June 17, 2015; Accepted for publication July 1, 2015; Published Online (www.bioelecmed.org) August 17, 2015.*

extent possible. By acknowledging the risks, we can offset and move past them—by architecting smart and secure solutions from the start of concept development, by placing safeguards around the critical aspects of connected systems and isolating them appropriately and by fostering collaborations of the right expertise at every developmental step.

Together, let's design well to be well.

## DISCLOSURE

The author declares that she has no competing interests as defined by *Bioelectronic Medicine*, or other interests that might be perceived to influence the results and discussion reported in this paper.

Cite this article as: Masters M. (2015) Melissa Masters's response to "Imagining the Future of Medicine" commentary. *Bioelectron. Med*. 2:53–4.