Medical Device Cybersecurity
A Guide for HTM Professionals

Edited by
Stephen L. Grimes, FACCE, FAIMBE, FHIMSS
Axel Wirth, CPHIMS, CISSP, HCISPP
ABOUT THE EDITORS

Stephen L. Grimes, FACCE, FAIMBE, FHIMSS, is principal consultant in Strategic Healthcare Technology Associates, LLC in Boston, MA. He is a fellow of the American Institute of Medical and Biological Engineering (AIMBE), of the Health Information and Management Systems Society (HIMSS) and the American College of Clinical Engineering (ACCE), where he is also a past president. He has been a prolific writer and speaker on medical device security for nearly 20 years and for over 40 years has served variously as director of clinical engineering at academic medical centers and in management and consulting roles in independent service organizations. He now consults in the areas of HTM strategic and operational issues, technology convergence, security and risk management associated with medical devices and systems, compliance, and quality management.

Axel Wirth, CPHIMS, CISSP, HCISPP, is a distinguished healthcare architect for Symantec Corp. In his role, he provides strategic vision and technical leadership, serving in a consultative role to healthcare providers, industry partners, and health technology professionals. Drawing from over 30 years of international experience in the industry, Mr. Wirth supports healthcare organizations with solving their critical security, privacy, compliance, and IT management challenges. He is an active participant in industry organizations and a frequent speaker at conferences, forums, and webcasts on subjects such as cybersecurity, medical device security, mobile health infrastructure, compliance automation, IT infrastructure optimization, and other healthcare-specific topics. In recognition of his accomplishments, he has been awarded the “2018 ACCE/HIMSS Excellence in Clinical Engineering & IT Synergies Award.”
Medical Device Cybersecurity
A Guide for HTM Professionals

Edited by
Stephen L. Grimes, FACCE, FAIMBE, FHIMSS
Axel Wirth, CPHIMS, CISSP, HCISPP

PREVIEW COPY
This is a preview edition of an AAMI guidance document and is intended to allow potential purchasers to evaluate the content of the document before making a purchasing decision.

For a complete copy of this AAMI document, contact AAMI at +1-877-249-8226 or visit www.aami.org.
# Table of Contents

<table>
<thead>
<tr>
<th>Acknowledgments by the Editors</th>
<th>v</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td>1</td>
</tr>
<tr>
<td>Karl J. West</td>
<td></td>
</tr>
<tr>
<td>CHAPTER 1. Medical Device Cybersecurity: A Public Health Perspective</td>
<td>3</td>
</tr>
<tr>
<td>Dale Nordenberg, MD</td>
<td></td>
</tr>
<tr>
<td>CHAPTER 2. Objective and Scope of This Guide</td>
<td>7</td>
</tr>
<tr>
<td>Stephen L. Grimes, FACCE, FAIMBE, FHIMSS</td>
<td></td>
</tr>
<tr>
<td>Axel Wirth, CPHIMS, CISSP, HCISPP</td>
<td></td>
</tr>
<tr>
<td>CHAPTER 3. Cybersecurity Fundamentals</td>
<td>9</td>
</tr>
<tr>
<td>Axel Wirth, CPHIMS, CISSP, HCISPP</td>
<td></td>
</tr>
<tr>
<td>Introduction by Lee Kim, JD, FHIMSS, CISSP, CIPP/US</td>
<td></td>
</tr>
<tr>
<td>CHAPTER 4. Understanding the Patient Care Environment</td>
<td>29</td>
</tr>
<tr>
<td>Stephen L. Grimes, FACCE, FAIMBE, FHIMSS</td>
<td></td>
</tr>
<tr>
<td>Axel Wirth, CPHIMS, CISSP, HCISPP</td>
<td></td>
</tr>
<tr>
<td>Introduction by David S. Finn, CISA, CISM, CRISC</td>
<td></td>
</tr>
<tr>
<td>CHAPTER 5. Managing the Technical Environment and Infrastructure</td>
<td>35</td>
</tr>
<tr>
<td>John T. Rasmussen, MA, MBA</td>
<td></td>
</tr>
<tr>
<td>Introduction by Sue Schade, FCHIME, LCHIME, FHIMSS</td>
<td></td>
</tr>
<tr>
<td>CHAPTER 6. Understanding the Regulatory and Standards Environment</td>
<td>47</td>
</tr>
<tr>
<td>Michelle Jump, RAC, MS, CHA</td>
<td></td>
</tr>
<tr>
<td>Introduction by Suzanne Schwartz, MD, MBA</td>
<td></td>
</tr>
<tr>
<td>CHAPTER 7. Stakeholders and Their Roles, Responsibilities, Training, and Education in Cybersecurity</td>
<td>61</td>
</tr>
<tr>
<td>Anahi Santiago, CISM</td>
<td></td>
</tr>
<tr>
<td>Introduction by Stephen L. Grimes, FACCE, FAIMBE, FHIMSS</td>
<td></td>
</tr>
<tr>
<td>CHAPTER 8. Managing the Asset: Inventory and Configuration Management</td>
<td>73</td>
</tr>
<tr>
<td>Stephen L. Grimes, FACCE, FAIMBE, FHIMSS</td>
<td></td>
</tr>
<tr>
<td>Introduction by Purna Prasad, PhD, CCE</td>
<td></td>
</tr>
</tbody>
</table>

© AAMI

This is a preview edition of an AAMI guidance document and is intended to allow potential purchasers to evaluate the content of the document before making a purchasing decision. For a complete copy of this AAMI document, contact AAMI at +1-877-249-8226 or visit www.aami.org.
CHAPTER 9. Medical Device Cybersecurity Risk Assessment. ................. 79
Stephen L. Grimes, FACCE, FAIMBE, FHIMSS
Introduction by Todd Cooper

CHAPTER 10. Medical Device Cybersecurity Risk Mitigation: Establishing Effective Governance. ........................................... 97
Scot Copeland, BSITSEC, CBET, MCP, SEC+
Mike Busdicker, MBA, CHTM
Priyanka Upendra, BSBME, MSE, CHTM
Introduction by Jennifer L. Jackson, CCE, FACCE

CHAPTER 11. Medical Device Cybersecurity Risk Mitigation: Fundamentals of Securing Medical Devices. ........................................ 115
Axel Wirth, CPHIMS, CISSP, HCISPP
Benjamin Esslinger, CBET
Introduction by Michael McNeil

CHAPTER 12. Medical Device Cybersecurity Risk Mitigation: Incident Response. ................................................................. 133
Timothy Torres, MBA, CISSP-ISSMP, CISM, HCISPP, ITIL
Introduction by Denise Anderson

CHAPTER 13. Trends and Future Developments in Securing Medical Devices . . . 151
Ken Hoyme
Shankar Somasundaram
Introduction by Anita Finnegan

APPENDIX A. Terms and Definitions. ........................................... 165

APPENDIX B. Acronyms. .............................................................. 169

APPENDIX C. Further Reading. ................................................... 173

APPENDIX D. Cybersecurity Risk Management Flow Chart. ............ 185

APPENDIX E. Tools, Policies, and Procedures. ............................... 187
Examples of Medical Device Cybersecurity Tools, Policies, and Procedures:
Mayo Clinic
Introduction by Kevin McDonald
- Medical Device Risk Assessment: Vendor Packet Instructions and Deliverables
- Technology and Security Requirements for Vendors of Clinical Systems and Associated Services

Examples of Medical Device Cybersecurity Tools, Policies, and Procedures:
Scripps Health and Intermountain Healthcare
Introduction by Scot Copeland, BSITSEC, CBET, MCP, SEC+;
Priyanka Upendra, BSBME, MSE, CHTM; Mike Busdicker, MBA, CHTM
- Change Management Policy
- Firewall Administration Change Control Policy
- Computer Equipment Life Cycle Ownership, Tracking, and Management Policy
- Disposal, Transfer, Reuse, and Data Sanitization of Equipment Policy
- Network Medical Devices Operating System Vulnerability Management Policy
Acknowledgments by the Editors

Writing and editing a book is a project. And, as in most projects, in the end it is a team effort and can only succeed if all pull together. With that in mind, the editors wish to extend their sincere thanks to all contributors, whether they provided a brief topic introduction or an in-depth chapter or allowed us to use example policies and forms in an appendix. We know that whatever their contribution, it was a volunteer effort done in addition to job and personal demands. We are all most grateful; this guide is better because of their participation and sacrifice.

During the six-month production period of this guide, people changed jobs, relocated, recovered from injuries, dealt with government shutdowns, survived hurricanes and flooding, and traveled the globe. Yet, in the end, all came together and we were able to hand something to AAMI that we all can be proud of.

We also wish to thank AAMI for its leadership and commitment and its help with educating the industry, which in the end is part of the solution to this complex problem. AAMI is keenly aware of the challenge of medical device cybersecurity and has committed its extensive talent and resources to the education of the industry and to the development of tools, standards, and guidance that industry can use to solve these challenges.

We hope you find this guide useful and beneficial.

Stephen L. Grimes, FACCE, FAIMBE, FHIMSS
Principal Consultant
Strategic Healthcare Technology Associates, LLC

Axel Wirth, CPHIMS, CISSP, HCISPP
Distinguished Technical Architect,
U.S. Healthcare Industry
Symantec Corporation
With Thanks and Gratitude to the Contributors:

Denise Anderson
President and CEO
National Health Information Sharing and Analysis Center (NH-ISAC)

Mike Busdicker, MBA, CHTM
System Director,
Clinical Engineering Services
Intermountain Healthcare

Todd Cooper
President
Breakthrough Solutions Foundry, Inc.

Scot Copeland, BSITSEC, CBET, MCP, SEC+
Lead Clinical Systems Specialist
Scripps Mercy Hospital

Benjamin Esslinger, CBET
Manager, Biomedical Engineering
Eskenazi Health

David S. Finn, CISA, CISM, CRISC
EVP, Strategic Innovation
CynergisTek, Inc.

Anita Finnegan
Chief Executive Officer
Nova Leah, Ltd.

Ken Hoge
Director, Product and Engineering Systems Security
Boston Scientific

Jennifer L. Jackson, CCE, FACCE
Director, Connectivity
Masimo Corporation

Michelle Jump, RAC, MS, CHA
Principal Regulatory Affairs Specialist
Carestream Health

Lee Kim, JD, FHIMSS, CISSP, CIPP/US
Director, Privacy and Security Health Information and Management Systems Society (HIMSS)

Kevin McDonald
Director, Clinical Information Security
Mayo Clinic

Michael McNeil
Global Product Security and Services Officer
Philips Healthcare

Dale Nordenberg, MD
Executive Director and CEO
Medical Device Innovation, Safety & Security Consortium (MDISS)

Purna Prasad, PhD, CCE
Vice President and Chief Technology Officer
Northwell Health

John Rasmussen, MA, MBA
Vice President and Chief Information Security Officer
MedStar Health

Anahi Santiago, CISM
Chief Information Security Officer (CISO)
Christiana Care Health System

Sue Schade, FCHIME, LCHIME, FHIMSS
Principal
StarBridge Advisors

Suzanne B. Schwartz, MD, MBA
Associate Director for Science and Strategic Partnerships
Center for Devices and Radiological Health, U.S. Food and Drug Administration

Shankar Somasundaram
Chief Executive Officer
Asimily, Inc.

Timothy Torres, MBA, CISSP-ISSMP, CISM, HCISPP, ITIL
Senior Deputy Chief Information Security Officer
Sutter Health

Priyanka Upendra, BSBME, MSE, CHTM
CE Compliance Manager
Intermountain Healthcare

Karl J. West
Assistant Vice President and CISO
Intermountain Healthcare
Foreword

Karl J. West

If you’ve acquired this guide, I strongly suspect you share my concerns with the issue of medical device security. Medical devices, which have become progressively more microprocessor-based and connected, are increasingly relied upon by healthcare providers to deliver efficient and accurate care. You’re not wrong to be concerned about the security of these devices. The underlying cybersecurity risks and their impact on the safety and security of your patients, employees, and organization as a whole are real. This is why the sale and distribution of medical devices is strictly regulated so to assure their safety and effectiveness.

Many of these medical devices are proprietary, highly specialized, and automated systems for collecting, analyzing, and storing critical and sensitive medical data. Because of its value, the data on medical devices might be targeted directly by cybercriminals or, alternatively, it might become infected by malware targeting other adjacent vulnerable systems. Protecting the security of critical data is paramount to providing care to millions of Americans and is one of many security concerns that keep cybersecurity professionals up at night.

The authors of this guide represent a collective of adept cybersecurity professionals who feel similarly about the risks these devices represent and have chosen to share with you some practices that will help to mitigate risk and secure these important technologies. Their combined knowledge merges in this guide to assist you in navigating the current state of medical device security and guidance for the future. The guide is not a catchall work. Rather, it is an introduction to the risks these devices present, their importance to public health, the evolving patient care environment, the technical and infrastructure needed to protect them, and the importance of stakeholder engagement. The guide also presents an effective approach to risk mitigation and gives an insight into future trends in how medical device security can more effectively be addressed. A rich compendium of cybersecurity sources is also included in a comprehensive appendix. I recommend consulting these sources to further your security education. Cybersecurity, after all, is about people. The more knowledge we can gain as security professionals, executives, and clinicians, the better we can protect the digital healthcare ecosystem—and ultimately our patients.

I’ve spent 30 years in the cybersecurity industry, and I’ve seen the extreme changes that have occurred over time. In healthcare, technology has inundated and disrupted the industry over the past decade—to our great collective benefit. However, we can’t assure security as the foundation to reliable care delivery, patient safety, and the business of healthcare without a clear plan for mitigating medical device risks. That makes this guide even more valuable. I’m pleased to represent the cadre of professionals whose knowledge buoys this guide and the Association for the Advancement of Medical Instrumentation (AAMI) in introducing you to this guide and its content.

Whether you’re a cybersecurity professional or a concerned healthcare provider, it’s up to us to advance our knowledge and to advocate for medical device security for the paramount reasons of SAFETY and SECURITY. Assuring the security of our medical device ecosystem requires a collaborative effort of the entire healthcare team. Please use this guide as a stepping stone toward a solution to this problem. It is not a panacea, but an important step in the very right direction.
CHAPTER 1
Medical Device Cybersecurity: A Public Health Perspective
Dale Nordenberg, MD

INTRODUCTION
The Association for the Advancement of Medical Instrumentation (AAMI) medical device cybersecurity guide is an important new contribution to growing efforts to strengthen the cyber protection programs of our nation's healthcare system and to reduce cyber risk to patient populations, healthcare providers, and health technology companies. AAMI's efforts are a great example of a public health initiative in action.

As a physician and public health professional who has dedicated his career to advancing digital health and its associated infrastructure for the improvement of patient care and population health, it only took one conversation back in 2009 to understand that we had designed and delivered medical products and services without fully understanding all the consequences and risks. In the process of accelerating towards connected health, we substantially increased cybersecurity risks. We created a national biomedical device network, a network of networks, but we failed to practice cybersecurity hygiene, resulting in an extensive form of “digital promiscuity.”

The nation's healthcare technology management workforce is at the frontlines of efforts to combat and mitigate cyber risk. The multidisciplinary collaboration between clinical engineers, network engineers, and security engineers is well described in IEC 80001-1:2010 (adopted in the United States as ANSI/AAMI/IEC 80001-1:2010), one of the first technical standards dedicated to medical device cybersecurity.1 However, the breadth and depth of this public health challenge is so large and complex that the domains of expertise required to mitigate cyber risk in our health system extend beyond the three disciplines initially defined in IEC 80001-1. We must now address this newly appreciated, endemic, digitally mediated public health challenge with a comprehensive and robust public health initiative.

THE IMPORTANCE OF A PUBLIC HEALTH PERSPECTIVE
The mission of public health as defined by the American Public Health Association (APHA) is to “promote and protect the health of the people.” “Public health works to track disease outbreaks, prevent injuries and shed light on why some of us are more likely to suffer from poor health than others. The many facets of public health include speaking out for laws that promote smoke-free indoor air and seatbelts, spreading the word about ways to stay healthy.