CyberSecurity in Medical Devices

CONTENTS

About Us
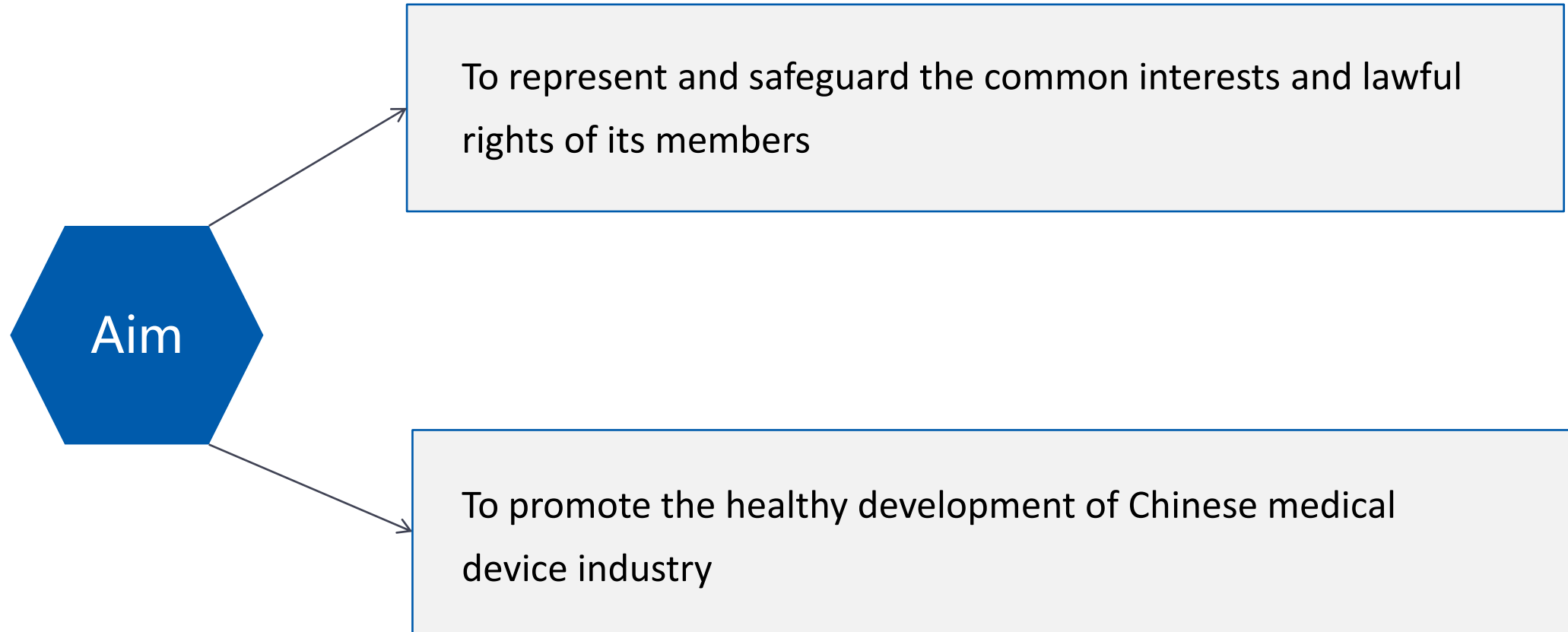
Chapter 1

Founded in 1991, China Association for Medical Devices Industry (CAMDI) is a national, industrial and nonprofit social organization that is formed, on a voluntary basis, by companies and individuals engaged in medical device R&D, manufacturing, management, investment, inspection and testing, certification consulting, and education & training. CAMDI has the corporative qualifications of social group.

CAMDI is under the supervision and administration of State-owned Assets Supervision and Administration Commission(SASAC).SASAC appoints and authorizes China Federation of Industrial Economics to manage CAMDI on his behalf. Meanwhile，CAMDI is under the professional guidance of relevant departments such as CFDA,MCA and NDRC.

About Us

Aim

To represent and safeguard the common interests and lawful rights of its members

To promote the healthy development of Chinese medical device industry

About Us

Chapter 1

27 full-time staff in the secretariat

45 branches and professional committees

4000 members and experts

About Us

Chapter 1
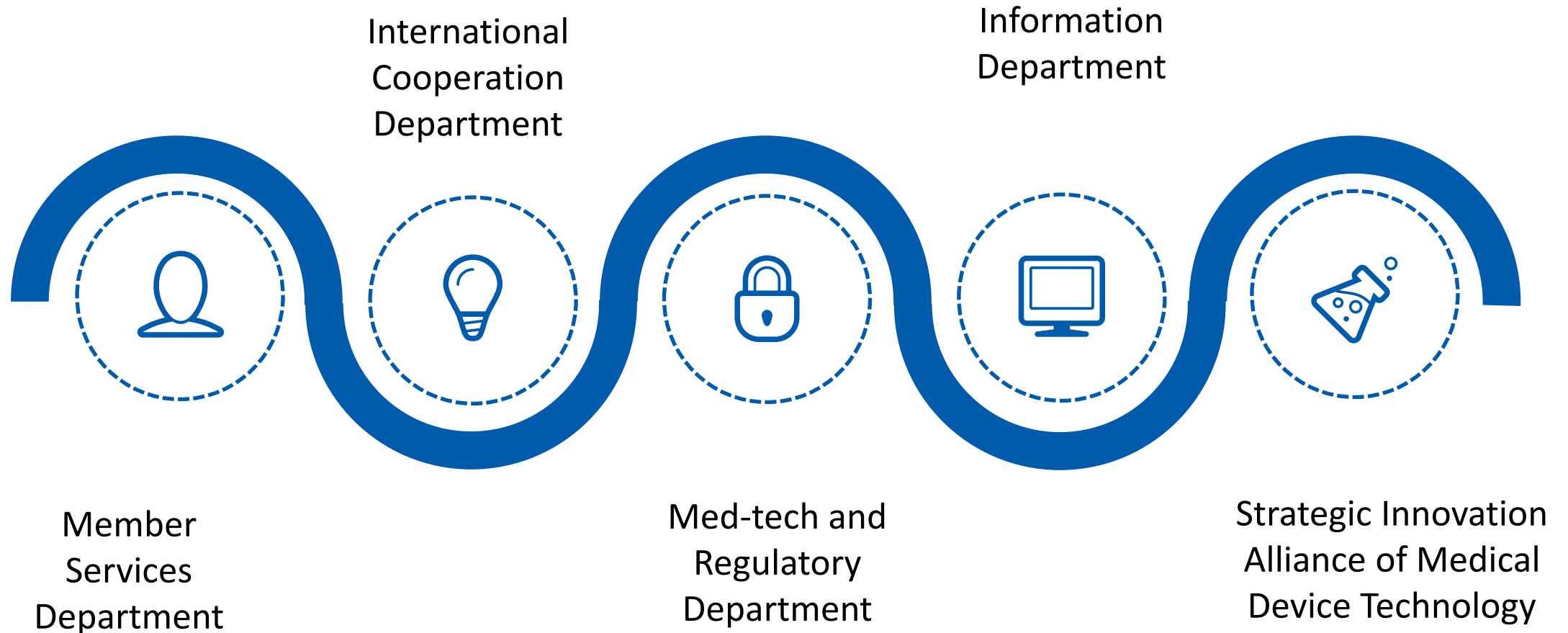
International
Cooperation
Department

Information
Department

Member
Services
Department

Med-tech and
Regulatory
Department

Strategic Innovation
Alliance of Medical
Device Technology

CONTENTS

CyberSecurity in Medical Devices

Chapter 2

- The use of software and network is becoming widely in medical device industry.

- CFDA has worked out several guidances on medical device software and cybersecurity.

- Guidance for cybersecurity in medical device is implemented from this year.

- The medical device industry on cybersecurity development still needs great improvement.

CyberSecurity in Medical Devices

Chapter 2

- The administration of cybersecurity in medical device is the supplement of administration of software in medical device.

- For medical device, by taking relevant methods of technical skills, to make sure the medical devices could be freed from network attack in order to keep the safety and effectiveness is the purpose and essence of cybersecurity.

CyberSecurity in Medical Devices

Chapter 2

- The compositing element of cybersecurity: network communication, information data(device data, health data, etc.), environmental invasion.

- The risk element of cybersecurity: unexpected operation of device, violation of information data and privacy, damage of patient or operator.

CyberSecurity in Medical Devices

Chapter 2

- The characteristic of cybersecurity:

- confidentiality, integrity, availability;

- authenticity, accountability, non-repudiation, reliability, etc.

CyberSecurity in Medical Devices

Chapter 2

- Rapid growth of IT technology leads to desynchronization between development of industry and the capability of solving risk.

- The globalization trend of the medical device versus the difference between different areas.

CyberSecurity in Medical Devices

Chapter 2

- Cyber security in medical device is a question involving multiple links, with whole life cycle of medical device.

- Different focus on the responsibilities between in or outside the medical device administration scope.

CyberSecurity in Medical Devices

Chapter 2

- Risk level of cybersecurity in medical device higher than traditional IT fields.

- Cybersecurity problems in medical device result in harder correction and longer period of validation.

CyberSecurity in Medical Devices

Chapter 2

- Terminology and definitions.

- Risk control and relevant consideration, both premarket approval and postmarket surveillance.

CyberSecurity in Medical Devices

Chapter 2

- Technical requirement of cybersecurity, and the capability of solving problems.

- Evaluation of the relevance and difference between medical device industry and other IT fields.

CyberSecurity in Medical Devices

Chapter 2

- Cybersecurity in medical device is an abstract and difficult problem. Both industry and governor in different countries is facing the challenge. The coordinating development of cybersecurity administration will make great progress in the globalized advancement.