

Westgate Cyber Security Limited

National Assembly for Wales

**Health and Social Care Committee – Medical
Technology inquiry**

Prepared By:
David Jones, Director

Effective Friday 5 October 2012

Contact information:

David Jones

Director, Westgate Cyber Security Limited

david.jones@westgatecybersecurity.com

TABLE OF CONTENTS

1	EXECUTIVE SUMMARY	4
	1.1 Background	4
	1.2 Overview and Summary	4
	1.3 Limitation of response	4
2	INFORMATION GOVERNANCE.....	6
3	EMERGING RISKS AND THREATS.....	7
4	CONCLUSION.....	8

1 EXECUTIVE SUMMARY

1.1 Background

The National Assembly Health and Social Care Committee is planning to conduct an inquiry into the appraisal of, and access to, medical technology.

Westgate Cyber Security Limited (Westgate) is a specialist Management Consultancy working in the area of information security.

1.2 Overview and Summary

Westgate is presenting the Committee some initial views on the subject of information security in relation to both existing and future medical technology.

Westgate's views can be summarized into the following three points

- *The pace of emerging technology in this domain is already significant, but will grow significantly in coming years, it already includes*
 - *Surgical robots*
 - *Tele-medicine devices*
 - *Portable information-gathering appliances (including consumer smart-phones)*
 - *Information systems*
 - *Data analytics, including the use of publicly available and pseudo-publicly available data (ranging from formal research data such GWASS studies to social media data-harvesting from sources such as Facebook)*
- The Information Governance issues will be increasingly important. Transparency of how the public perceive the use of the data presents a risk to up-take. Appropriate use of data, especially data-sharing protocols are critical. This issue is referred to as **Information Governance** below.
- There is a real and emerging threat from external factors. Conventionally referred to as "hacking", this threat requires a close understanding of the vulnerabilities of both physical devices and information systems. This issue is referred to as **Emerging Risks and Threats** below.

1.3 Limitation of response

This document only seeks to comment on the scope of the enquiry, not set out detailed evidence. Therefore the response is limited to raising and listing some of the key points only.

Furthermore, Westgate's response is limited to the area of Information Security only.

It does not include the following:

- Decision-making processes in NHS Wales

- Funding for technology
- Accessibility
- Appraisal of technology



2 INFORMATION GOVERNANCE

1. There are a number of Welsh Government systems, protocols and processes in place surrounding the governance of information.

These include, but are not limited to

- a. Data-sharing protocols (WASPI)
 - b. Formal Information Governance roles (the Caldicot Guardian, usually held by the Health Board's Medical Directors)
2. The issues of transparency are key. The public need to both understand and respect the processes surrounding the data.
 3. "Ownership" of medical information is an issue that is not sufficiently clear. Patients are service-users are right to think that the data on their health (effectively, their Medical Record) is owned by them, but the usual conventions of ownership are not in place.



3 EMERGING RISKS AND THREATS

Some of the most interesting developments currently taking place are in the area of physical Medical devices and tools. These range in complexity from small tele-medicine devices to fully functional surgical robots, capable of undertaking orthopaedic operations.

The threats and risks fall into two areas:

a. Internal Factors.

The failure of any kind of device poses clear problems of reliability and also reputational loss. Often these failures of hardware, software or communication technology are quality issues, which can be mitigated by quality assurance processes.

b. External Factors

This is a real and growing threat.

Within industries such as energy and transportation (collectively known as Critical National Infrastructure – CNI) there is already a high level of maturity around the issue of the risk from parties intent on external attack. Often this is referred to as Cyber-Terrorism.



4 CONCLUSION

Westgate hope that this review includes the issues surrounding information security and information governance.

Westgate will be pleased to submit detailed written evidence to the committee and give verbal evidence.