

FOR IMMEDIATE RELEASE



## STUDY: HOSPITAL IT ANXIOUS ABOUT GROWING MOBILE SECURITY THREATS, SAYS SPYGLASS CONSULTING GROUP

82% hospitals surveyed expressed concerns that mobile technology deployments are not adequately protected to address increased risk of cybersecurity attacks

**MENLO PARK, CA, August 22, 2016.** Today, Spyglass Consulting Group released its most recent healthcare study, **Point of Care Communications for Nursing 2016**. The study shows that 82 percent of hospitals surveyed expressed grave concerns about their ability to support and protect mobile devices, patient data, and the hospital's technology infrastructure as a result of the growing threat of cybersecurity attacks.

Mobile devices including smartphones and tablets can introduce vulnerabilities to the hospital's network and infrastructure through attack vectors that include:

- Malware - designed to penetrate networks, steal information, and cover up its tracks,
- Blastware - designed to destroy or disable a system when detected, and
- Ransomware - designed to block access to a computer system until money is paid.

Hospitals surveyed were concerned about personally-owned mobile devices used by physicians and advanced practice nurses, because many end users

- have inadequate password protection,
- lack security software to thwart an attack,
- rely upon unsecured SMS messaging for clinical communications which often included patient health information, and
- widely use public WiFi and cellular networks that could easily compromise their device, data and communications.

Hospitals surveyed also were concerned about hospital-owned and managed mobile devices used by nurses, ancillary healthcare professionals, and other mobile hospital workers. "Despite increased investments in mobile device management solutions and secure text messaging solutions, cybercriminals have become more sophisticated and knowledgeable about the capabilities and vulnerabilities of existing security products, and the strategies and tools used by hospital IT to detect a potential intrusion," said Gregg Malkary, Spyglass Consulting Group.

HIPAA privacy rules require hospitals to closely guard and protect patient health information, such as patients' names, birth dates, social security numbers, diagnoses, tests, physicians' names, and insurance information. Hospitals found guilty of data breaches can be fined upwards of \$1.5 million per incident and be required to notify the local media if the breach involves more than 500 patient records. Approximately 25 percent of data breaches originate from mobile devices.

**ADDITIONAL HIGHLIGHTS OF THE POINT OF CARE COMMUNICATIONS FOR NURSING 2016 REPORT:**

**HOSPITAL IT INVESTMENT PRIORITIES ARE PIVOTING TOWARD MOBILE COMMUNICATIONS**

Seventy-one percent of hospitals surveyed regard mobile communications as an emerging investment priority driven by the adoptions of new patient centered care models and value-based purchasing.

**LARGE-SCALE ENTERPRISE-WIDE DEPLOYMENTS ARE FOCUSING ON THE MOBILE HOSPITAL WORKER**

Thirty-eight percent of hospitals surveyed had invested in a smartphone-based communications platform to support clinical communications with an average size deployment of 624 devices. Fifty-two percent of them have expanded their deployments beyond clinical messaging to support other mobile hospital workers.

## **ABOUT SPYGLASS' POINT OF CARE COMMUNICATIONS FOR NURSING 2016 REPORT**

**Point of Care Communications for Nursing 2016** presents the findings of an end-user market study focused on the current state of mobile communications adoption by nurses across the United States.

The report uncovers strong opinions regarding the market opportunities and challenges for hospitals and health systems who are considering large-scale deployments of Smartphones and mobile unified communications to help nurses, physicians, ancillary care workers, and medical support staff to streamline communications, improve team-based collaboration, and enhance care coordination across the healthcare continuum.

**Point of Care Communications for Nursing 2016** is an outgrowth of a similar study published by Spyglass in March 2014 entitled Point of Care Communications for Nursing 2014. Content for Point of Care Communications for Nursing 2016 was derived from more than 100 in-depth interviews with IT and healthcare professionals working in hospital-based environments who are technically competent and representative of a broad range of medical specialties, organization types, and organization sizes.

The telephone interviews were conducted over a three-month period starting in March 2016. The purpose of the interviews was to identify the needs and requirements for communications at point of care through discussions about existing workflow inefficiencies in communicating with care team members, current usage models for mobile communications devices and solutions, and barriers for widespread mobile communications adoption.

Spyglass also evaluated key vendor product offerings and identified early adopter organizations that successfully deployed point of care solutions.

The **Point of Care Communications for Nursing 2016** report is targeted at:

- **software and hardware vendors, systems integrators and management consulting groups** who are selling hardware, applications and services into the healthcare industry,
- **healthcare administrators and IT executives** who are making strategic decisions to fund clinical information technology solutions,
- **clinicians** who are involved in informatics and clinical system evaluation, and
- **investment banking and private equity investors.**

The complete market study, "**Healthcare Without Bounds: Point of Care Communications for Nursing 2016,**" is available for \$2,495 (USD) from Spyglass Consulting Group at [www.spyglass-consulting.com](http://www.spyglass-consulting.com).

## ABOUT SPYGLASS CONSULTING GROUP



**Spyglass Consulting Group** is a market intelligence firm and consultancy focused on the nexus of information technology and healthcare. Spyglass offers products and services in customer and market intelligence, strategic partnership development, product marketing and investment due diligence. Spyglass' current research is entitled **Healthcare without Bounds** that focuses on the current and future potential of mobile computing and wireless technologies within the healthcare industry.

Spyglass customers include more than 140 leading high technology vendors, management consulting organizations and healthcare providers including **Cisco, IBM, Microsoft, Intel,**

**Hewlett Packard, Johnson & Johnson, Pfizer, Siemens, GE Healthcare, Philips Medical, Sprint,** and **Kaiser Permanente.**

**Gregg Malkary** is the **founder** and **Managing Director** of **Spyglass Consulting Group**. He has more than 20 years' experience in the high technology industry working with Fortune 2000 companies to help them use information technology for competitive advantage. Malkary has domain expertise in mobile computing, wireless and broadband technologies with direct experience in the healthcare, hospitality, manufacturing, communications and entertainment markets.

Prior to founding **Spyglass Consulting Group** in 2002, Malkary was an Associate Partner at **Outlook Ventures**, a venture capital firm focused on early stage investments in enterprise software and communications companies. Previously, Malkary was the Director of Strategic Planning for **Exodus Communications** where he was responsible for identifying, evaluating and executing growth initiatives for Exodus in the managed Web-hosting marketplace. Malkary has also held consulting and senior management roles in business development, strategic planning and product marketing for public and private technology companies including **IBM, Hewlett Packard, Accenture, Silicon Graphics** and **Skytel Communications.**

Malkary frequently speaks at regional and national conferences focused on mobile computing, wireless technologies and healthcare related issues. Numerous industry publications have written about and quoted Malkary including the Wall Street Journal, CIO, Business 2.0, MIT Technology Review, Network World and eWeek.

Malkary is an honors graduate of **Brown University** having earned a MS and BA in Computer Science. He was awarded the prestigious North American Philips Corporation Fellowship for his graduate research work in graphical simulation environments.

For additional information about this study, please contact Gregg Malkary at [gmalkary@spyglass-consulting.com](mailto:gmalkary@spyglass-consulting.com).

### Contact:

Gregg Malkary, Managing Director  
Spyglass Consulting Group  
(650) 575-9682  
[gmalkary@spyglass-consulting.com](mailto:gmalkary@spyglass-consulting.com)