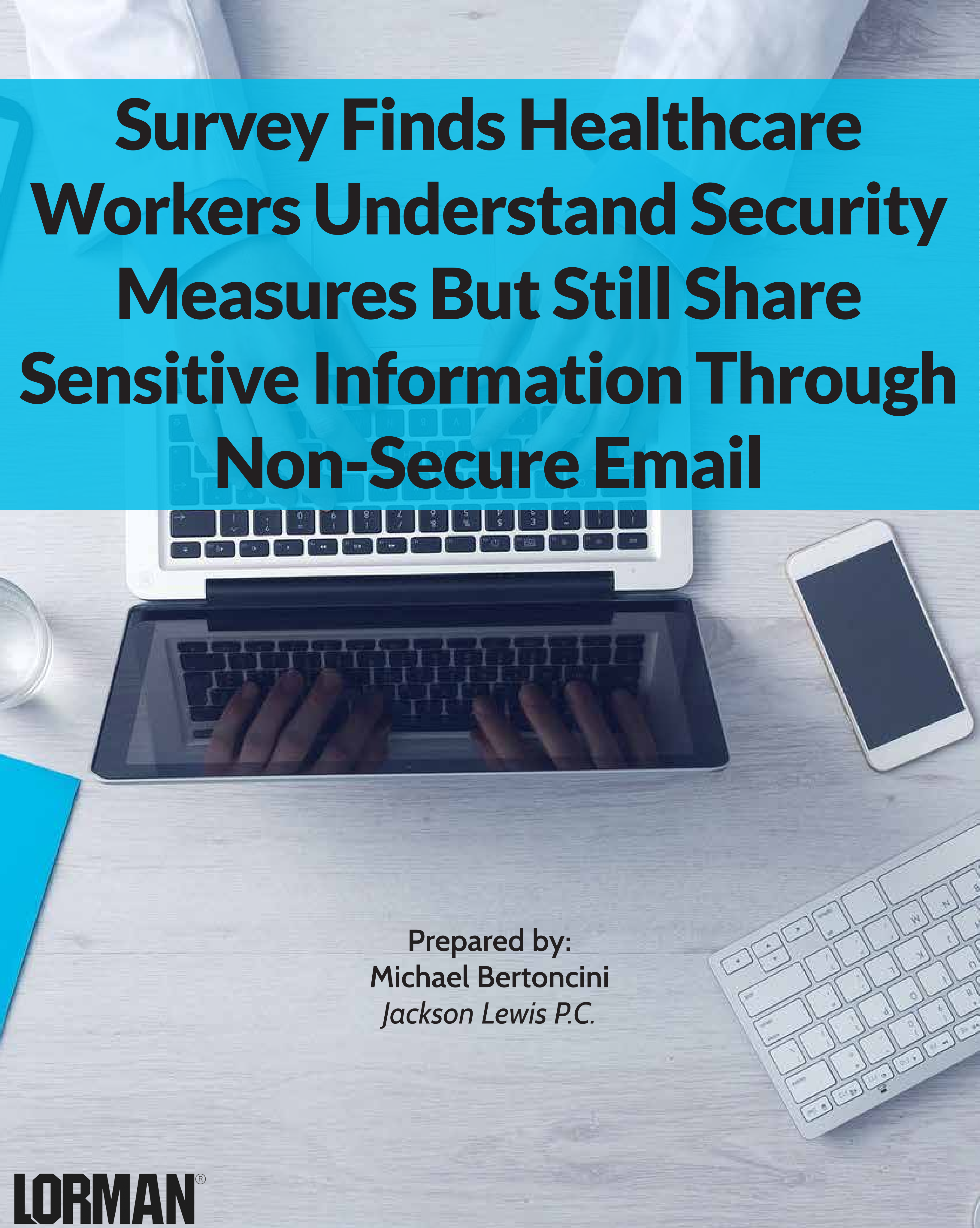

Survey Finds Healthcare Workers Understand Security Measures But Still Share Sensitive Information Through Non-Secure Email

Prepared by:
Michael Bertoncini
Jackson Lewis P.C.

LORMAN®
Published on www.lorman.com - November 2018

Survey Finds Healthcare Workers Understand Security Measures But Still Share Sensitive Information Through Non-Secure Email

Written by Michael Bertoncini – 6/13/18

According to reports on a recent survey, the vast majority of healthcare workers share sensitive medical information using non-secure email. The survey, conducted by Kickstand Communications, reportedly found that 87% of healthcare workers surveyed admitted to this practice. These results echo other reports finding that employees and others with access to an organization's confidential information may pose the greatest risk to data security.

As reported by HealthITSecurity.com, key findings from the survey include:

- Healthcare workers are 36 percent more likely to share regulated data such as patient information and credit card information via non-secure methods such as email than those working in financial services;
- 10 percent of healthcare employees admit they do not abide by their employer's security rules;
- More than one-quarter of respondents share sensitive data, documents, and information externally using personal sync and share services like Dropbox;
- Across industries, 29 percent of respondents admit sharing intellectual property via non-secure email externally; and
- When deciding how to send sensitive documents, 60 percent of respondents across industries said they simply do what is easiest.

The survey reportedly also found that an overwhelming number of healthcare employees understand their employers' information security policies and how to use the secure communications tools provided to them. Yet, a majority reportedly indicated that they do whatever is easiest when they need to transfer data and 64 percent said when it comes to sharing data, email is the easiest tool.

The survey results suggest that healthcare providers' data security efforts cannot end at training employees to use their communications tools. Rather, these efforts must include programs to create a culture of information security. This can include elements such as:

- Reminders of the reasons the security measures have been put in place;
- Exploring ways to make secure communications systems easier to use;
- Soliciting employee feedback on ways to make secure communications more efficient; and
- Auditing the use of non-secure methods of communication.

As scrutiny from regulators increases and plaintiffs' lawyers bring new claims based on data breaches, healthcare employers and employers across all industries need to be sure they walking the walk and not just talking the talk on information security.

It is critical that businesses ensure their employees have greater awareness of the sensitivity of the personal information they acquire, handle and transport, and receive training about how to be more cautious handling it. The Jackson Lewis Privacy, e-Communications and Data Security team can help your organization with employee training and implementing appropriate procedures to address these types of risks.

Below are additional Jackson Lewis resources that address employee handling of sensitive personal information in the healthcare industry:

- **Dealing with Data Breaches: Health Net Suit Highlights Need for Effective Security Incident Procedures and Training**
- **Blue Cross/Blue Shield Data Breach Highlights Need for Employee Training/ Awareness**

The material appearing in this website is for informational purposes only and is not legal advice. Transmission of this information is not intended to create, and receipt does not constitute, an attorney-client relationship. The information provided herein is intended only as general information which may or may not reflect the most current developments. Although these materials may be prepared by professionals, they should not be used as a substitute for professional services. If legal or other professional advice is required, the services of a professional should be sought.

The opinions or viewpoints expressed herein do not necessarily reflect those of Lorman Education Services. All materials and content were prepared by persons and/or entities other than Lorman Education Services, and said other persons and/or entities are solely responsible for their content.

Any links to other websites are not intended to be referrals or endorsements of these sites. The links provided are maintained by the respective organizations, and they are solely responsible for the content of their own sites.