HIPAA

Gerry Blass and Susan A. Miller, JD

Business Intelligence and Big Data

What are the HIPAA Privacy and Security Impacts?

By Gerry Blass and Susan Miller, JD

THE TERMS *business intelligence* and *big data* are the new buzzwords for using tools and techniques to sort and resort data for a secondary or other use within a business.

The definition of business intelligence describes it as a set of techniques and tools for the transformation of raw data into meaningful and useful information. Big data means that there are more and more healthcare data and that healthcare data are more connected than ever before. With the advent of health information exchanges (HIEs); accountable care organizations (ACOs) now, Meaningful Use regulations, and more extensive use of data aggregators (e.g., registries), healthcare data are now used to help in the provision of medical care, as well as in predicting when and where an event might happen.

Because we are talking about healthcare information, we must also talk about protected health information (PHI) and the HIPAA-HITECH-OMNIBUS (Health Insurance Portability and Accountability Act, Health Information Technology for Economic and Clinical Health Act) Privacy, Security, and Breach Notification Rules. Business intelligence and big data analysis that includes PHI and its use and disclosure must be reviewed against the HIPAA security and privacy requirements and the breach notification requirements.

If the business intelligence and big data analysis includes using PHI for treatment, payment, and healthcare operations (TPO), then current policies, procedures, plans, and processes are most likely sufficient but should be updated accordingly. For example, if your organization is using its data to determine if a type of drug is being used effectively and efficiently, then the HIPAA definitions treatment and healthcare operations will likely cover the use and disclosure of PHI for these purposes, again with appropriate updates to include the aspects of business intelligence and big data.

The same is true for business intelligence and big data uses and disclosures for research purposes. Current policies, procedures, plans, and processes are most likely sufficient, whether the HIPAA privacy requirements of the Common Core are used individually or together.

It is when your organization uses and/or discloses PHI for other purposes than TPO and research that other HIPAA-HITECH-OMNIBUS Privacy and Security standards and implementation specifications need to be reviewed. We suggest the following areas be considered:

De-identification (45 CFR 164. 514)
Limited Data Set (45 CFR 164. 514)
Public Health (45 CFR 164.512)
Deceased Individuals (45 CFR 164.502)
Marketing (45 CFR 164.501)
Business Associate Agreements (45 CFR 164.308(b), 45 CFR 164.504(e))
All HIPAA Security Rule standards

In any analysis, it is important to remember to begin with the definitions in the HIPAA requirements, such as with marketing, as the HIPAA definitions are part of the scope of the HIPAA requirements.

In previous *JHIM* columns, the authors discussed the need to conduct an ePHI vulnerability assessment and determine controls, gaps, risk, and risk mitigation. The assessment applies to locations where ePHI is in transit and at rest. Potential locations to analyze include servers, workstations, portable devices, email, WIFI, cloud hosting, and more. We can provide a full list upon request. The ePHI assessment should also include a detailed risk analysis drill down for business intelligence and big data controls, gaps, risk, and risk mitigation. It is simply a numbers game, and the numbers of risk areas keep growing, which results in larger risks for breach when proper controls are not in place.

Also note that the National Institute of Standards and Technology (NIST) has released its Big Data Framework for comment. The framework is organized by volumes, including:

Volume 1: Definitions
Volume 2: Taxonomies
Volume 3: Use Cases and General Requirements
Volume 4: Security and Privacy
Volume 5: Architectures White Paper Survey
Volume 6: Reference Architecture
Volume 7: Standards Roadmap.

The NIST Big Data Interoperability Framework may be found on the NIST Big Data Public Working Group page at: http://bigdatawg.nist.gov/V1_output_docs.php

In conclusion, any PHI used in business intelligence and big data will need to

THE TERMS BUSINESS INTELLIGENCE and big data are the new buzzwords for using tools and techniques to sort and resort data for a secondary or other use within a business.

comply with all the related HIPAA Privacy, Security, and Breach Notification requirements and must therefore be analyzed to even a greater degree when it comes to uses and disclosures, controls, and risk. It is even more important today for healthcare organizations and Business Associates to implement a *culture of compliance*, with a major focus on Data Governance and Risk Management. Remember that it is a numbers game, and the numbers of locations of PHI in transit and at rest keep increasing at a rapid pace. **JHIM**

Gerry Blass is the President & CEO of ComplyAssistant. Blass has over 35 years of experience in healthcare IT and compliance. Blass provides IT and compliance consulting services and software (also called ComplyAssistant) that automates the management and documentation of healthcare compliance activities. To learn more, visit www.complyassistant.com.

Susan A Miller, JD has 40 years of professional leadership experience spanning college teaching, biochemistry research, and law. Since 2002, Miller has provided independent consulting and legal services to numerous healthcare entities including NIST (National Institute of Standards and Technology) and HHS (U.S. Department of Health and Human Services). She has co-authored two OCR (Office of Civil Rights, HHS) audit protocol prep-books, HIPAA (Healthcare Insurance Portability and Accountability Act) Security Audit Prep Book, and HIPAA Breach & Privacy Audit Prep Book. She can be reached at TMSAM@aol.com. They are published at http://www.malverngroup.com/New_Publications.html. Blass and Miller are co-founders of HIPAA 411, a LinkedIn group.

Journal of Healthcare Information Management® (ISSN 1943-734X) is published quarterly by the Healthcare Information and Management Systems Society (HIMSS). Subscription to this publication is a benefit of membership in HIMSS. Application to mail at Periodicals postage rate is pending in Chicago, IL, and additional mailing offices.

Statements and opinions appearing in articles and departments of the journal are those of the authors and do not necessarily reflect the position of HIMSS. Canadian Agreement #40648621.

NOTE: Starting with volume 16, Number 2, each volume of *Journal of Healthcare Information Management*® begins with the WINTER issue.

U.S. SUBSCRIPTIONS cost $69.00 for individuals and $104.00 for institutions, agencies, and libraries. Standing orders are accepted. There is no sales tax on U.S. subscriptions. Canadian residents, add GST and any local taxes.

INTERNATIONAL SUBSCRIPTIONS cost $109 for individuals and $144 for institutions.

EDITORIAL QUESTIONS AND PERMISSION REQUESTS should be directed to Nancy Vitucci, Senior Manager, HIMSS Media, 33 West Monroe St., Chicago, IL 60603-5616, (312) 915-9238, (312) 915-9288 (fax), nancy.vitucci@himssmedia.com

INTERACTIVE ADVERTISING AND REPRINTS
For interactive advertising opportunities, contact Karen Diekmann, HIMSS Media, 207-791-8720 at karen.diekmann@himssmedia.com
A full reprint of this publication is available for $59. Please send in your request to Ian Maurer, The YGS Group, (717) 505-9701 x941, Ian.Maurer@theygsgroup.com

ADDRESS CHANGES should be sent to Healthcare Information and Management Systems Society, 33 West Monroe St., Chicago, IL 60603-5616.

Published in the United States of America.