

Criminal Healthcare Cyberattacks on the Rise

Healthcare data breaches have occurred more frequently over the past few years.¹ With the cyberattacks over the last year on Premera Blue Cross, Community Health Systems, Anthem Inc., and CareFirst, millions of Americans have had their information potentially exposed to hackers.² Not only have the cyberattacks occurred more frequently, but the number of patients exposed has also grown exponentially.³ In January 2015 alone, two different healthcare cyber security breaches were discovered, affecting more than 90 million Americans, compared to only two million affected individuals in the entirety of 2012.⁴ Even more troubling, the number of *criminally motivated* breaches, in contrast to *employee negligence* breaches, has risen to its highest level yet, and now accounts for 45% of all healthcare data breaches.⁵ These criminal attacks are most commonly committed by nation-state actors, malicious insiders, and thieves who physically steal information.⁶ In a 2015 study conducted by the security firm *Ponemon Institute*, 90% of the nearly 200 business associates and healthcare organizations surveyed experienced at least one data breach, and 40% of those surveyed experienced more than five breaches in the past two years.⁷

Healthcare data breaches have increased exponentially over the past few years, likely due to the extremely valuable information that healthcare entities possess, including names, social security numbers, credit card information, birthdays, addresses, and various medical data points.⁸ This information can be used to steal an individual's identity to commit fraud or any number of other malicious acts. Many attacks have not resulted in the collection of social security numbers or credit card information, but have resulted in the collection of other personal information.⁹ However, in the largest healthcare cyber security breach to date, which affected approximately 80 million Anthem, Inc. customers, hackers accessed the customers' personal information, including social security numbers and employment information.¹⁰ Fortunately for Anthem customers, to date, no identity theft has been discovered from the breach, so there has not yet been a violation of the *Health Insurance Portability and Accountability Act* (HIPAA).¹¹

In August 2013, the U.S. Department of Health and Human Services (HHS) Office of Civil Rights Director Leon Rodriguez reported that the majority of data breaches occur because companies have failed to perform an adequate risk assessment and apply the findings to

their current practices in order to strengthen those practices.¹² However, likely due in part to the increasing number of data breaches, healthcare entities have begun improving their security systems and developing stronger monitoring programs to check for weaknesses in their systems and respond to breaches more quickly.¹³ In 2013, 69% of healthcare organizations reported that they had some kind of security plan for data breaches, which was 7% higher than in 2012, and 27% of organizations reported that they were developing a plan.¹⁴ But indications suggest that these improvements may not be occurring fast enough or functioning effectively enough. The 2015 *Ponemon Institute's* study found that approximately 58% of healthcare organizations believed their policies and procedures were effective at preventing data theft, but only 49% have the technology to effectively prevent the breaches, and 33% believe they have enough resources to prevent and detect breaches.¹⁵ Without adequate resources and functioning technology, the personal information of patients may still be at risk of cyberattack.

In 2013, HHS implemented its *HIPAA Final Omnibus Rule*, which clarifies the conditions under which entities must report patient data breaches, and fines the companies up to \$1.5 million per violation, depending on their level of negligence.¹⁶ According to Director Rodriguez, this rule is expected to increase the number of HIPAA breach cases that result in fines.¹⁷ However, by introducing stronger penalties for failure to safeguard patient information, the *Omnibus* rule may positively affect patients by encouraging healthcare organizations to better protect patient information from cyberattack.

The upward trend in healthcare data breaches is not likely to slow down going forward, considering the technology and information available to hackers. Consequently, healthcare organizations may have an even stronger motivation than before to develop effective security policies and procedures to protect patient information. The significant breach of Anthem's database, which affected 80 million individuals, caused a "wake up call" for consumers who are beginning to show a greater concern for the safekeeping of their personal information.¹⁸ This heightened public awareness of the data breaches, coupled with the HIPAA *Omnibus* rule, may fuel the efforts of companies to protect the personal information of their consumers and monitor their privacy systems for problems.¹⁹

-
- 1 “HIPAA Data Breaches Climb 138 Percent” By Erin McCann, Healthcare IT News, February 6, 2014, <http://www.healthcareitnews.com/news/hipaa-data-breaches-climb-138-percent> (Accessed 6/3/15).
 - 2 “Up to 1.1 Million Customers Could be Affected in Data Breach at Insurer CareFirst” By Matthew Goldstein and Reed Abelson, The New York Times, May 20, 2015, http://www.nytimes.com/2015/05/21/business/carefirst-discloses-data-breach-up-to-1-1-million-customers-affected.html?_r=0 (Accessed 6/3/15); “Health Care Data Breaches Have Hit 30M Patients and Counting” By Jason Millman, The Washington Post, August 19, 2014, <http://www.washingtonpost.com/blogs/wonkblog/wp/2014/08/19/health-care-data-breaches-have-hit-30m-patients-and-counting/> (Accessed 6/3/15).
 - 3 “Slideshow: Biggest Health Data Breaches” By Erin McCann, Healthcare IT News, March 17, 2015, <http://www.healthcareitnews.com/slideshow/slideshow-top-10-biggest-hipaa-breaches?page=11> (Accessed 6/3/15).
 - 4 “Massive Breach at Health Care Company Anthem, Inc.” By Elizabeth Weise, USA Today, February 5, 2015, <http://www.usatoday.com/story/tech/2015/02/04/health-care-anthem-hacked/22900925/> (Accessed 6/3/15); “Infographic: Biggest Healthcare Data breaches of 2012” By Erin McCann, Healthcare IT News, December 21, 2012, <http://www.healthcareitnews.com/news/infographic-biggest-healthcare-data-breaches-2012> (Accessed 6/3/15).
 - 5 “Healthcare Data Breaches From Cyberattacks, Criminals Eclipse Employee Error for the First Time” By Kelly Jackson Higgins, Dark Reading, May 7, 2015, <http://www.darkreading.com/attacks-breaches/healthcare-data-breaches-from-cyberattacks-criminals-eclipse-employee-error-for-the-first-time/d/d-id/1320315> (Accessed 6/3/15).
 - 6 *Ibid.*
 - 7 “Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data” Ponemon Institute, May 2015, http://ipa.idexperts.com/acton/attachment/6200/f-037a/1/-/-/-/5th%20Annual%20Privacy%20and%20Security%20of%20Healthcare%20Data%20Report.pdf?cm_mmc=Act-On%20Software_-_email_-_Thank%20you%20for%20downloading%20the%20Fifth%20Annual%20Benchmark%20Study%20on%20Privacy%20and%20Security%20of%20Healthcare%20Data_-_Click%20here%20to%20download%20the%20report.&sid=232C-UrdKz (Accessed 6/3/15), p. 1.
 - 8 “Health Care Data Breaches Have Hit 30M Patients and Counting” By Jason Millman, The Washington Post, August 19, 2014, <http://www.washingtonpost.com/blogs/wonkblog/wp/2014/08/19/health-care-data-breaches-have-hit-30m-patients-and-counting/> (Accessed 6/3/15).
 - 9 Goldstein and Abelson, May 20, 2015.
 - 10 “Massive Breach at Health Care Company Anthem, Inc.” By Elizabeth Weise, USA Today, February 5, 2015, <http://www.usatoday.com/story/tech/2015/02/04/health-care-anthem-hacked/22900925/> (Accessed 6/3/15).
 - 11 *Ibid.*
 - 12 McCann, “HIPAA Data Breaches Climb 138 Percent,” February 6, 2014.
 - 13 Millman, August 19, 2014.
 - 14 *Ibid.*
 - 15 Ponemon Institute, May 2015, p. 3.
 - 16 “New Rule Protects Patient Privacy, Secures Health Information” HHS, January 17, 2013, <http://www.hhs.gov/news/press/2013pres/01/20130117b.html> (Accessed 6/3/15); “Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the HITECH Act and the GINA; Other Modifications to the HIPAA Rules” 78 Federal Register Vol. 78 No. 17 (January 25, 2013), p. 5565-5702.
 - 17 McCann, “HIPAA Data Breaches Climb 138 Percent,” February 6, 2014.
 - 18 Millman, August 19, 2014.
 - 19 *Ibid.*



(800) FYI - VALU

*Providing Solutions
in the Era of
Healthcare Reform*

Founded in 1993, HCC is a nationally recognized healthcare economic financial consulting firm

- [HCC Home](#)
- [Firm Profile](#)
- [HCC Services](#)
- [HCC Experts](#)
- [Clients & Projects](#)
- [HCC News](#)
- [Upcoming Events](#)
- [Contact Us](#)
- [Email Us](#)

HEALTH CAPITAL

CONSULTANTS (HCC) is an established, nationally recognized healthcare financial and economic consulting firm headquartered in St. Louis, Missouri, with regional personnel nationwide. Founded in 1993, HCC has served clients in over 45 states, in providing services including: valuation in all healthcare sectors; financial analysis, including the development of forecasts, budgets and income distribution plans; healthcare provider related intermediary services, including integration, affiliation, acquisition and divestiture; Certificate of Need (CON) and regulatory consulting; litigation support and expert witness services; and, industry research services for healthcare providers and their advisors. HCC's accredited professionals are supported by an experienced research and library support staff to maintain a thorough and extensive knowledge of the healthcare reimbursement, regulatory, technological and competitive environment.



Robert James Cimasi, MHA, ASA, FRICS, MCBA, CVA, CM&AA, serves as Chief Executive Officer of **HEALTH CAPITAL CONSULTANTS (HCC)**, a nationally recognized healthcare financial and economic consulting firm headquartered in St. Louis, MO, serving clients in 49 states since 1993. Mr. Cimasi has over thirty years of experience in serving clients, with a professional focus on the financial and economic aspects of healthcare service sector entities including: valuation consulting and capital formation services; healthcare industry transactions including joint ventures, mergers, acquisitions, and divestitures; litigation support & expert testimony; and, certificate-of-need and other regulatory and policy planning consulting.

Mr. Cimasi holds a Masters in Health Administration from the University of Maryland, as well as several professional designations: Accredited Senior Appraiser (ASA – American Society of Appraisers); Fellow Royal Institution of Chartered Surveyors (FRICS – Royal Institute of Chartered Surveyors); Master Certified Business Appraiser (MCBA – Institute of Business Appraisers); Accredited Valuation Analyst (AVA – National Association of Certified Valuators and Analysts); and, Certified Merger & Acquisition Advisor (CM&AA – Alliance of Merger & Acquisition Advisors). He has served as an expert witness on cases in numerous courts, and has provided testimony before federal and state legislative committees. He is a nationally known speaker on healthcare industry topics, the author of several books, the latest of which include: "[Accountable Care Organizations: Value Metrics and Capital Formation](#)" [2013 - Taylor & Francis, a division of CRC Press], "[The Adviser's Guide to Healthcare](#)" – Vols. I, II & III [2010 – AICPA], and "[The U.S. Healthcare Certificate of Need Sourcebook](#)" [2005 - Beard Books]. His most recent book, entitled "[Healthcare Valuation: The Financial Appraisal of Enterprises, Assets, and Services](#)" was published by John Wiley & Sons in 2014.

Mr. Cimasi is the author of numerous additional chapters in anthologies; books, and legal treatises; published articles in peer reviewed and industry trade journals; research papers and case studies; and, is often quoted by healthcare industry press. In 2006, Mr. Cimasi was honored with the prestigious "[Shannon Pratt Award in Business Valuation](#)" conferred by the Institute of Business Appraisers. Mr. Cimasi serves on the Editorial Board of the Business Appraisals Practice of the Institute of Business Appraisers, of which he is a member of the College of Fellows. In 2011, he was named a Fellow of the Royal Institution of Chartered Surveyors (RICS).



Todd A. Zigrang, MBA, MHA, ASA, FACHE, is the President of **HEALTH CAPITAL CONSULTANTS (HCC)**, where he focuses on the areas of valuation and financial analysis for hospitals, physician practices, and other healthcare enterprises. Mr. Zigrang has over 20 years of experience providing valuation, financial, transaction and strategic advisory services nationwide in over 1,000 transactions and joint ventures. Mr. Zigrang is also considered an expert in the field of healthcare compensation for physicians, executives and other professionals.

Mr. Zigrang is the author of the soon-to-be released "[Adviser's Guide to Healthcare – 2nd Edition](#)" (AICPA, 2014), numerous chapters in legal treatises and anthologies, and peer-reviewed and industry articles such as: [The Accountant's Business Manual](#) (AICPA); [Valuing Professional Practices and Licenses](#) (Aspen Publishers); [Valuation Strategies; Business Appraisal Practice](#); and, [NACVA QuickRead](#). Additionally, Mr. Zigrang has served as faculty before professional and trade associations such as the American Society of Appraisers (ASA); the National Association of Certified Valuators and Analysts (NACVA); the Physician Hospitals of America (PHA); the Institute of Business Appraisers (IBA); the Healthcare Financial Management Association (HFMA); and, the CPA Leadership Institute.

Mr. Zigrang holds a Master of Science in Health Administration (MHA) and a Master of Business Administration (MBA) from the University of Missouri at Columbia. He is a Fellow of the American College of Healthcare Executives (FACHE) and holds the Accredited Senior Appraiser (ASA) designation from the American Society of Appraisers, where he has served as President of the St. Louis Chapter, and is current Chair of the ASA Healthcare Special Interest Group (HSIG).



John R. Chwarzinski, MSF, MAE, is Senior Vice President of **HEALTH CAPITAL CONSULTANTS (HCC)**. Mr. Chwarzinski holds a Master's Degree in Economics from the University of Missouri – St. Louis, as well as, a Master's Degree in Finance from the John M. Olin School of Business at Washington University in St. Louis. Mr. Chwarzinski's areas of expertise include advanced statistical analysis, econometric modeling, and economic and financial analysis.



Jessica L. Bailey, Esq., is the Director of Research of **HEALTH CAPITAL CONSULTANTS (HCC)**, where she conducts project management and consulting services related to the impact of both federal and state regulations on healthcare exempt organization transactions and provides research services necessary to support certified opinions of value related to the Fair Market Value and Commercial Reasonableness of transactions related to healthcare enterprises, assets, and services. Ms. Bailey is a member of the Missouri and Illinois Bars and holds a J.D., with a concentration in Health Law, from Saint Louis University School of Law, where she served as Fall Managing Editor for the Journal of Health Law and Policy.



Richard W. Hill, III, Esq. is Senior Counsel of **HEALTH CAPITAL CONSULTANTS (HCC)**, where he manages research services necessary to support certified opinions of value related to the Fair Market Value and Commercial Reasonableness of transactions related to healthcare enterprises, assets, and services, and conducts analyses of contractual relationships for subject enterprises. Mr. Hill is a member of the Missouri Bar and holds a J.D., with a concentration in Health Law, from Saint Louis University School of Law.