



NOVEMBER 2016

LHCC MEMBERS

- Robelyn Abadie
- Jeff Albright
- Diane Davidson
- Rachel Durel, DDS
- Rusty Eckel, PT
- William L. Ferguson, PhD
- John F. Fraiche, MD
- Lisa Gardner
- Lauren Gleason
- Arnold M. Goldberg
- Anthony M. Grieco, MD, MBA
- Faye Grimsley, PhD, CIH
- Korey Harvey
- Linda P. Hawkins
- Hedy S. Hebert
- Marlon D. Henderson, DDS
- The Honorable Mike Huval
- Jesse Lambert, PsyD
- Eva Lamendola, OD
- Jesse McCormick
- Jennifer McMahon
- Rachel Moore, MD
- Barbara Morvant
- Andrew Muhl
- B. Ronnell Nolan, HIA, CHRS
- John Overton
- Daniel Paquin
- Ed Parker
- Katie Parnell
- Clay Pinson
- Theresa Ray
- Debra Rushing
- James C. "Butch" Sonnier, BS, DC
- Chris Vidrine
- Bryan Wagner
- The Honorable Rick Ward, III
- Thomas N. Wright



FROM THE EXECUTIVE DIRECTOR

Welcome to the LHCC's quarterly newsletter! We hope to bring to you information beyond the minutes of our meetings, highlighting some of the most pressing issues in healthcare that we continue to study and address.

We also have a new feature to share with you. As the LHCC remains committed to increasing its knowledge on key issues in the health care delivery system faced by consumers, we'll soon offer a link on our web site available to the public for comment and participation that provides us with an opportunity to make recommendations to the Commission.

Our next LHCC meeting is approaching soon! Make sure you save the date -- Friday, November 4th. We will meet at 9:00 am at the Louisiana Department of Insurance to hear from Dr. SreyRam Kuy, Chief Medical Officer and Medicaid Medical Director at the Louisiana Department of Health and Hospitals. Dr. Kuy will speak to us on Medicaid Expansion and the unique challenges in serving this new population. Additionally we will hear from Stephanie Mills, MD, MHCM, President and CEO of Franciscan Health and Wellness Services, Inc. who will be bringing our audience up to speed on cost effectiveness of preventive health.

Thank you for your interest and I look forward to seeing you all at our next meeting!

Crystal M. Campbell

LHCC Executive Director



The LHCC Looks at Cybersecurity

Julie Freeman

The National Transportation and Safety Board conducts studies on plane crashes to assess the probability of future flying risks. Consumer Reports utilize crash test dummies to assist the public in making informed decisions on the safety of vehicles, and building codes establish a set of standards to ensure the structural safety of buildings routinely occupied for school, work and entertainment.

But not all businesses have a set of cybersecurity standards in place to ensure the security of a business' electronic network data.

According to the 2016 Research Report released by the Ponemon Institute, among 600 IT leaders and small and medium-sized businesses that were surveyed, only 14 percent of the companies represented in the study rated their ability to mitigate cyber risks and attacks as “highly effective.”

And not all states are statutorily required by law to develop cybersecurity strategies for business entities.

While cybersecurity legislation has been introduced in at least 25 states, requiring government to implement security practices and otherwise provide incentives for cybersecurity education, only a handful of states—Florida, Georgia, Indiana, Utah and Wyoming-- have been successful in passing legislation for government to implement security practices, according to a 2016 Cybersecurity Legislation Report, provided by the National Conference of State Legislatures.



The LHCC members listen intently as Henry Overton reiterates the importance of businesses having cybersecurity standards in place.

The high-profile data breach against the nation's second largest insurer, Anthem, followed by a rapid succession of other organizations victimized by security hacks in 2015, still reverberates throughout cyberspace serving as an epic cautionary tale on the importance of cybersecurity. And as cyber criminals become more sophisticated, businesses faced with evolving security threats against its networks must be ready and armed with a solid pre-emptive plan of

action that begins with a compliance plan and moves forward with the implementation and re-evaluation of risk management strategies and practices to fight the war on cyber-attacks.

Henry Overton, President and Co-Founder of Turn Key Solutions, L.L.C., has provided extensive security expert technology services for over 200 small to medium sized business and healthcare-related clients. He advises instituting a cybersecurity plan is a marathon, not a sprint.

“You have to assemble your team and include your staff leaders, not just your IT department. Delegate wisely but stay engaged,” says Overton.

He recommends a 5-step risk management process:

1. IDENTIFICATION of Risk Areas – such as insufficient backups, incomplete antivirus protection, disgruntled employees and mobile devices.
2. ASSESSMENT of Risks- Do a real risk assessment that involves your staff, not limited to IT
3. CREATION of a Risk Management Plan prioritizing risks
4. IMPLEMENTATION of risk controls
5. PERIODIC RE-EVALUATION of the success of implemented safety measures

With the ferocity and frequency of cyber-attacks, the deployment of high level safeguards is no longer an option but a necessity. IT Program Specialist Gabriel Tate recommends firewalls, intrusion prevention systems and intrusion defense systems as a first line of defense against network breaches, and back up measures such as data encryption and keeping servers up to date with the latest security patches. But, even with these safeguards in place, the possibility of a security breach still exists and, if it happens, the strongest defenses won't remediate the crippling loss and damage sustained by a business, including but not limited to business network shut down, identity theft, damage to a business' reputation and costly lawsuits.

And the chances of your business facing a security breach are ostensible. A 2016 study released by the Ponemon Institute, estimates there is a 24% chance of the likelihood of a breach happening over 24 months. The average total cost of a breach is \$4 million, up by 29 percent since 2013, and the cost per record breach for health care organizations is \$355 per record breach.

Another extra layer of defense for the security of electronic data is with a cyber-liability insurance policy. While a commercial insurance policy provides general liability coverage to protect the business from property damage or injury, it does not cover cyber risks such as identity theft, business interruption and other risks that may be covered by a cyber-liability insurance policy.



Speaker Henry Overton of Turn Key Solutions, L.L.C. speaking on Cybersecurity

According to the National Association of Insurance Commissioners, a cyber-liability insurance policy might cover one or more of the following:

- Loss of confidential information by allowing or failing to prevent unauthorized access to computer systems
- Costs associated with a privacy breach such as consumer notification, customer support and costs of providing credit monitoring services to affected consumers.
- Costs associated with restoring, updating or replacing business assets stored electronically
- Business interruption and extra expense related to security or privacy breach
- Liability associated with libel, slander, copyright infringement, product disparagement or reputational damage to others when the allegations involve a business website, social media or print media
- Expenses related to cyber extortion or cyber terrorism
- Coverage for expenses related to regulatory compliance or billing errors, physician self-referral proceedings and Emergency Medical Treatment and Active Labor Act proceedings

The immediate advantages of having a stand-alone cyber insurance policy as reported in a January 2015 Bloomberg BNA's World Data Protection Report, include providing companies with an immediate solution to transfer first and third party costs of a data breach and providing crisis management in response to the security breach.

In summary, while a company can't predict when and if it will face a security data breach, it can be prepared to mitigate the damages through security and compliance efforts of an assembled team who actively participate in a risk management program, coupled with purchase of a cyber-liability insurance policy.



Speakers Nadine Robin and Brian Richmond of the LHCQF speaking on Louisiana Information Exchange and DHH's Electronic Health Record Incentive Plan (with Henry Overton and Rep. Mike Huval)

The LHCC also heard from the Louisiana Health Care Quality Forum (LHCQF) on the Louisiana Health Information Exchange, DHH's Electronic Information Exchange and Electronic Health Record Incentive Plan.

With the passage of the American Reinvestment & Recovery Act by President Obama in 2009, funding was granted for health care information technology and the

building of a statewide health information exchange. The second grant established by the Louisiana Regional Extension Center. It was funded to assist providers, particularly those in primary care independent practices, to implement a new health care infrastructure, defined as "Meaningful Use," (MU) promulgated by CMS for providers' use of certified electronic health

record (EHR) technology in ways that measurably improve patients' quality and value, according to Nadine Robin of the LHCQF.

“As of last year in working with the Office of Public Health, 70 statewide parish health units have made the successful transition to electronic health records, managing thousands of patients within a single system,” she said.

Congress also passed a new set of regulations created under the Medicare Access and CHIP Reauthorization Act (MACRA). MACRA combines the Medicare Meaningful use (MU), Physician Quality Reporting System (PQRS), and Value-Based Modifier (VBM) into MIPS payment adjustments, a Merit-Based Incentive Payment Model system moving from a pay-for-performance to pay-for-service activities at the Medicare level, according to Ms. Robin.

“With a program roll out introduction in 2017, and a full roll out in 2018, the overall effect will enable providers who have higher MIPS scores to receive a slightly higher payment rate on specific services than providers who score lower and receive lower reimbursement rates,” she said.



Another exchange that manages a secure a secure HIPAA compliant messaging system between providers and patients is the Louisiana Health Information Exchange (LaHIE).

Speakers Nadine Robin and Brian Richmond of the LHCQF speaking on Louisiana Information Exchange and DHH's Electronic Health Record Incentive Plan (with Henry Overton)

The purpose of this exchange is to facilitate the process of providers accessing patient records across different care settings in order to make better-informed decisions. There are more than 300 participants in this health exchange across Louisiana for various health care facilities, according to LHCQF's Chief Technology Officer, Brian Richmond.

“LaHIE has information on approximately 4.5 million patients and has collected information from different participants through the exchange since 2011,” he said.

Board Member Spotlight

Chairperson John F. Fraiche, M.D



Family Background:

- A New Orleans native, Dr. Fraiche currently resides in Baton Rouge
- Married for 42 years to Donna D. Fraiche, past Chair of the Louisiana Health Care Commission
- Father of two doctors and three grandsons

Education:

- Graduate of Jesuit High School in New Orleans, LSU in Baton Rouge and LSU Medical School in New Orleans
- Family practice residency completed at Earl K. Long Hospital in Baton Rouge

Employment:

- President of and family practitioner of St. Elizabeth Physicians in Gonzales, a multi-specialty group servicing Ascension Parish
- Serves as a doctor for a number of chemical plants and other facilities
- Has served as Coroner of Ascension Parish since 1987

From Dr. Fraiche:

“As a physician and parent to two practicing physicians, I have a passion for the future landscape of our healthcare system that is further enhanced by their common desire to make a difference in the lives of others while addressing today’s most pressing issues in health care. My hobbies include attending the opera and symphonies, cooking, and collecting French wine. I also have a great appreciation for contemporary art and once owned an art gallery in New Orleans.”