THE MONTHLY PUBLICATION FOR CAP MEMBERS

CAPsules

COOPERATIVE OF AMERICAN PHYSICIANS

Cyber Risk: Why You Are a Target and How to Avoid Being the Next Victim

A Special to *CAPsules*

A data breach happened to Anthem Blue Cross. Then, St. Joseph Health System. Sutherland Healthcare Solutions. And Hurley Medical Center.

And on February 5, Hollywood Presbyterian Medical Center's network was hit with ransomware. Everything at the hospital had to happen with pens, paper, and telephones for 10 days. The hospital had no real choice but to pay the $17,000 the hackers demanded.

If this can happen at a medium-sized institution with good IT – and they could not defuse this kind of attack – you can be sure it can happen anywhere. As Elliott Frantz, CEO of Virtue Security noted, "This incident really sheds light on how weak the cores of many providers' internal infrastructure are. It is very common for hospitals to have a large number of outdated and vulnerable systems on the network."

There is an undeniable pattern. Hackers are targeting the healthcare industry with a vengeance, and no target is too big or too small. This trend will affect everyone from Anthem Blue Cross to the smallest offices. Is your practice ready?

There is nearly a one-in-five chance you'll be hit

According to the most recent data, 15 to 20 percent of the breaches and loss of HIPAA personal health information have hit smaller practices. Why? Smaller practices are data-rich targets that are typically poorly defended.

At small practices, security is "important but not urgent." It is rarely in the budget. Small practices rarely have dedicated IT staff, which means systems are not fully patched and up to date. Furthermore, everybody is multitasking. Hackers know all it takes is one distracted click to crash an entire practice for days or even weeks.

It is worth 10 to 20 times more to hack your practice than to hack a bank

Healthcare records are wonderfully complete: credit card information, insurance data, full names, addresses, and even social security numbers. Hackers can sell a single healthcare record for 10 to 20 times more than what they might be able to get for other financial data.

And once someone has that information, there's a lot they can do with it. Someone who does not have health insurance can get a needed surgery done and the real patient will not even realize it until they see a surgery he or she never had mysteriously appear in the Explanation of Benefits mail.

Russian ransomware: 90,000 infections a day

A recent variety of ransomware called "Locky" is not very sophisticated, but it is spreading fast. British analyst Kevin Beaumont, during a recent interview with *Forbes* magazine, said more than 100,000 PCs were infected the day before the interview, while his contact at Fujitsu suggests as many as 90,000 infections were taking place per day. Beaumont said at one point, connections to his domain peaked at five requests per second.

Small practices are an easy target for ransomware "spearphishing." It is easy to get a list of doctors online, and send emails with malware attachments

continued on page 2

March 2016

Continued from page 1

to every practitioner in the area. If a hacker asked each physician for $15,000, it would be possible to make a lot of money very quickly. If your data is not backed up, you really have no choice but to pay what the crooks demand.

The health of your healthcare practice depends on security. No small practice can afford to be out of business for days or weeks at a time. Make sure you take the proper precautions.

10 WAYS TO PROTECT YOUR PRACTICE

1. Install end-point security software, including antivirus, antispyware, and antimalware, which updates regularly.
2. Keep your operating system fully up to date. Ideally you should aim to use the very latest version of software, especially if you are using Microsoft. If that's not at minimum use versions that Microsoft still supports (XP is not one of them), and make sure you regularly install important updates. Remember that investing in good security is always cheaper than cleaning up after a breach. Consider having your system audited and penetration tested by an external vendor once a year.
3. Use encryption with passwords on all computers, laptops, and smartphone devices. Change those passwords every 30 to 60 days – and forbid sharing them or leaving a post-it note with the password on the keyboard.
4. Make sure you have Business Associate Agreements with any vendor who has access to your data. If a data breach happens through a vendor, it is your responsibility.
5. Implement workplace policies to control data and implement a consistent approach to data security (again, you should absolutely forbid sharing passwords and login information).
6. Establish clear rules and regulations regarding the use of personal devices brought to the workplace.
7. All correspondence with patients should be done through a secure email system. Note that if it is free – for example, Gmail – it is *not* secure.
8. Make sure all files are securely backed up on a daily basis. But be careful not to store more data than is required. In some cases, firms unthinkingly pile up years worth of data. Ask your lawyer about data retention requirements.
9. Create a to-do data recovery and disaster plan. Make one person in charge of this plan: If it is everybody's responsibility, it will become no one's responsibility.
10. Provide training to staff on guidelines and HIPAA, HITECH, and email phishing techniques.

March 2016

CAP Board Reduces Its Size

Pursuant to the authority approved by the membership in July 2015, the Cooperative of American Physicians, Inc. Board of Directors has reduced the size of the Board from 15 directors to 11.

At the CAP Board meeting on January 29, four Directors who also serve on the Mutual Protection Trust Board of Trustees, Juan Carlos Cobo, MD, Charles Steinmann, MD, Phillip Unger, MD, and Glenn Weissman, MD, resigned from their positions on the CAP Board and will remain on the MPT Board. The CAP Board then voted to reduce the number of directors to 11 under CAP Bylaws Section 4.2.1.

How Much Could You Afford to Pay If Your Patient Data Was Hacked?

The healthcare industry continues to be one of the main targets for cybercrime. In 2015, the number of breaches and patient records stolen or compromised continued to grow. There are two main reasons for the increase in the number of healthcare Personal Health Information (PHI) and Personal Individual Information (PII) being targeted.

One is because of the type of information that hospitals and medical practices store in both electronic and paper formats. Medical practices store information such as health insurance, health data, social security numbers, as well as ages and addresses that can be sold for a much higher amount than other stolen data. The second reason is the information is not always as secure as other industries, such as retail and banking.

Prior to 2015, the most frequent causes of lost or stolen patient information was because of loss of electronic devices such as a laptops, phones, or portable drives. In 2015, the most frequent cause of lost patient data was actually because of hackers who are able to hack into databases and steal medical records.

Of course, the best situation would be to take steps to prevent data breach of your patient information and comply with HIPAA and HITECH regulations. And because CAP recognizes that even when the best precautions are taken a breach can still occur, CAP Physicians Insurance Agency, Inc. provides a CyberRisk Insurance policy for all of our members to protect their practice in case there is a data breach involving the PHI or PII of their patients.

The policy provides protection in the areas listed below as well and gives guidance and direction as to what you need to do in the event you do experience a breach:

- Multimedia Liability
- Security and Privacy Liability
- Privacy Regulatory Defense and Penalties
- Network Asset Protection
- Cyber Extortion
- Cyber Terrorism
- Crisis Management Expenses and Breach Response Costs

The limits of coverage are $50,000 per claim with notification costs outside of the policy limit. One of the most costly parts of data breach is the requirements of having to notify each patient who may have had his or her record breached. The average notification costs can run from $5 to $30 per notification, depending on the level of the breach. CAP CyberRisk policy will pay for 5,000 notifications outside the policy limit of $50,000 per claim.

CAP Physicians Insurance Agency, Inc. is working to help physicians understand the risks of data breach and what can be done to protect their practice by providing valuable tips on how to prevent and mitigate a breach. You also may want to consider purchasing an additional CyberRisk policy that provides $1,000,000 limits. If you are interested in obtaining more information or would like to consider purchasing higher limits, please contact us at CAPAgency@CAPphysicians.com.

CAP PHYSICIANS INSURANCE®
License No. 0F97719

March 2016

Cooperative of American Physicians, Inc. and Mutual Protection Trust

Statement of Privacy Obligations

This Statement of Privacy Obligations ("Statement") sets forth the policy of the Cooperative of American Physicians, Inc., Mutual Protection Trust, and their respective departments, committees, subsidiaries and affiliates (collectively, "CAP"), to safeguard the privacy and security of protected health information disclosed to CAP by, or created, maintained, sent, or received by CAP on behalf of CAP Members and Participants, in accordance with the Standards for Privacy of Individually Identifiable Health Information (Privacy Regulations) under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health Act ("HITECH"), and their amendments, regulations, and regulatory guidance (collectively, "the HIPAA rules"). Depending upon the circumstance, CAP may or may not be acting in the capacity of a "Business Associate" with respect to the use or disclosure of Protected Health Information ("PHI") received from a CAP Member or Participant acting as a "Covered Entity." (Capitalized terms herein are defined in the HIPAA rules.) This Statement is intended to apply in the circumstance where the HIPAA rules, in addition to other laws, apply. Notwithstanding the foregoing, CAP's adoption of this Statement should not be construed as an admission by CAP that it is acting in the capacity of a Business Associate with respect to such PHI or as a waiver of CAP's rights to object to such designation.

A. Permitted Uses and Disclosures of Protected Health Information

CAP provides services for the operations of CAP Members and Participants that may involve the use and disclosure of PHI. These services may include, among others, quality assessment, quality improvement, outcomes evaluation, protocol and clinical guidelines development, review of the competence or qualifications of healthcare professionals, evaluation of practitioner and provider performance, training programs to improve the skills of healthcare practitioners and providers, credentialing, performance or arrangement of medical reviews, arrangement or direct provision of legal services, performance or arrangement of audits to improve compliance, resolution of internal grievances, placement of stop-loss and excess of loss insurance, and other functions necessary to perform these services (collectively, "Services"). Except as otherwise specified herein, CAP may make any uses and disclosures of PHI necessary to perform their obligations under the MPT Agreement and to provide additional CAP benefits. All other uses or disclosures not authorized or permitted or required by law are prohibited. Moreover, CAP may disclose PHI for the purposes authorized by this Statement: (i) to its employees, subcontractors, and agents, in accordance with Section B.6 below; (ii) as directed by the CAP Members and Participants; or (iii) as otherwise permitted by the terms of this Statement.

Additionally, unless otherwise limited herein, CAP is permitted to make the following uses and disclosures:

1. Use PHI in its possession for its proper management and administration and to fulfill any present or future legal responsibilities of CAP, provided that such uses are permitted under state and federal confidentiality laws.

2. Disclose PHI in its possession to third parties for the purpose of its proper management and administration or to fulfill any present or future legal responsibilities of CAP, provided that (i) the disclosures are required by law; or (ii) CAP has received from the third party written assurances regarding its confidential handling of such PHI as required under 45 C.F.R. §164.504(e)(4).

3. Aggregate PHI of CAP Members and Participants that CAP has in its possession with PHI of other CAP Members and Participants, provided that the purpose of such aggregation is to provide the CAP Members and Participants with data analyses relating to the healthcare operations of the CAP Members and Participants. Under no circumstances may CAP disclose PHI of one CAP Member or Participant to another CAP Member or Participant absent the explicit authorization of the CAP Members and/or Participants concerned.

continued on page 5

Continued from page 4

4. De-identify any and all PHI provided that the de-identification conforms to the requirements of 45 C.F.R. § 164.514(b), and further provided that the CAP Member and/or Participant is sent the documentation required by 45 C.F.R. § 164.514(b), which shall be in the form of a written assurance from CAP. Pursuant to 45 C.F.R. § 164.502(d)(2), de-identified information does not constitute PHI and is not subject to the terms of this Statement.

B. Responsibilities of CAP

With regard to the use and/or disclosure of PHI, CAP hereby agrees to do the following:

1. Use and/or disclose PHI only as permitted or required by the Agreement or this Statement or as otherwise required by law.

2. Report to CAP Members and/or Participants in writing: (i) any use and/or disclosure of the PHI that is not provided for by the Agreement or this Statement of which CAP becomes aware; (ii) any breach of unsecured PHI that CAP discovers, as required by 45 CFR 164.410; and/or (iii) any Security Incident of which CAP becomes aware. The timing of the report will be consistent with CAP's legal obligations under the Breach Notification Rule and applicable state law.

This Statement constitutes ongoing notice to CAP Members and Participants of unsuccessful Security Incidents that do not represent substantial risks to PHI, such as pings on our firewall, unsuccessful log-on attempts, or access to encrypted information without access to a key, and no further reporting is required.

3. Following the discovery of a breach of unsecured PHI as defined under the HIPAA Rules, cooperate with and assist the CAP Member or Participant of such breach in complying with the breach notification requirements under 45 CFR § 164.410 without unreasonable delay.

4. Mitigate, to the extent practicable, any harmful effect that is known to CAP of an unauthorized use and/or disclosure of PHI by CAP.

5. Use reasonable and appropriate administrative, technical, and physical safeguards that protect the confidentiality, integrity, and availability of electronic PHI that CAP creates, receives, maintains, or transmits on behalf of the CAP Members and Participants.

6. To the extent commercially practicable, require all of its subcontractors and agents that undertake to perform the Services that CAP performs under the Agreement and that receive or use, or have access to PHI under the Agreement to agree, in writing, to adhere to the same restrictions and conditions on the use and/or disclosure of PHI that CAP has adopted pursuant to this Statement.

7. Unless prohibited by attorney-client and other applicable legal privileges or in violation of CAP's contractual and other legal obligations to CAP Members and Participants, make available all records, books, agreements, policies, and procedures relating to the use and/or disclosure of PHI to the Secretary of HHS for purposes of determining compliance with the Privacy Regulations.

continued on page 6

Continued from page 5

8. Honor any request from a CAP Member or Participant for information to assist in responding to an individual's request for an accounting of disclosures of PHI by CAP. However, should a CAP Member or Participant be asked for an accounting of the disclosures of an individual's PHI in accordance with 45 C.F.R. § 164.528, such accounting shall not include any disclosures by CAP to carry out the CAP Member's and/or Participant's healthcare operations or any other excepted disclosures described in 45 C.F.R. § 164.528.

9. Upon notification of individual's request to a CAP Member or Participant for access and/or amendment of PHI disclosed to CAP, assist the CAP Member or Participant to comply with their duties to the extent applicable under 45 C.F.R. §§ 164.524 and 164.526. However, CAP recognizes that, in some instances, PHI in CAP's possession is not part of a Designated Record Set as that term is defined by 45 C.F.R. § 164.501; and/or the information is exempt from access and amendment under 45 C.F.R. §§ 164.524(a) and 164.526(a)(2); and/or a request for access would violate or conflict with other contractual and legal rights of the CAP Members and Participants; and/or the request for amendment could be considered tampering with evidence in a civil or administrative proceeding.

C. Obligations of CAP Members and Participants

Each CAP Member and Participant:

1. Agrees to timely notify CAP, in writing, of any arrangements between the CAP Member and/or Participant and the individual that is the subject of PHI that may impact the Use and/or Disclosure of that PHI by CAP under this Statement.

2. Shall not request CAP to use or disclose PHI in any manner that would not be permissible under the HIPAA Rules if done directly by the CAP Member or Participant.

3. Represents that, to the extent the CAP Member and/or Participant provides PHI to CAP, such PHI is the minimum necessary PHI for the accomplishment of CAP's purpose.

4. Represents that, to the extent the CAP Member and/or Participant provides PHI to CAP, the CAP Member and/or Participant has already obtained the consents, authorizations and/or other forms of legal permission required under the HIPAA Rules and any other applicable law.

5. Has implemented reasonable and appropriate measures to ensure that PHI and electronic PHI are disclosed, provided, or transmitted to CAP only in a secure manner including through the use of a technology or methodology specified by the Secretary in the guidance issued pursuant to the HITECH Act, or if such guidance is not issued within the time specified in the HITECH Act, by a technology standard that renders PHI unusable, unreadable, or indecipherable to unauthorized individuals.

D. Terms and Termination

1. Upon termination of the relationship with CAP, the protections of this Statement will remain in force and CAP shall:

   a) Retain only that PHI which is necessary for CAP to continue its proper management and administration or to carry out its legal responsibilities;

   b) Continue to use appropriate safeguards and comply with the HIPAA Rules with respect to electronic PHI to prevent use or disclosure of the PHI, for as long as CAP retains the PHI;

   c) Not use or disclose the PHI retained by CAP other than for the purposes for which such PHI was retained and subject to the same conditions set forth in Section A above;

   d) Return to the CAP Member or Participant, or where agreed upon, destroy the PHI retained by CAP when it is no longer needed by CAP for its proper management and administration or to carry out its legal or contractual responsibilities.

2. The obligations of CAP under this Statement shall survive the termination of the relationship with CAP.

Civil Justice Reformer John Sullivan Dies

MICRA

March 2016

John Sullivan, the former president of the Civil Justice Association of California (CJAC) and a longtime leader in the fight against frivolous lawsuits, has passed away at the age of 73.

The organization was formed in 1979 as a principal supporter of the then newly-passed Medical Injury Compensation Reform Act (MICRA). In the years since, CJAC's legislative operations and appellate advocacy have promoted a legal system that supports patient access to care and a fair environment for business and employers.

CJAC, originally known as the Association for California Tort Reform, was led by Sullivan from 1995 to 2010. A fixture in Sacramento Capitol politics for almost 40 years, Sullivan passed away on February 20 from complications of cancer. During his long career navigating the halls of the state Legislature, Sullivan was respected by colleagues and opponents alike. Nancy Peveri, legislative director of the Consumer Attorneys of California, told the *Capitol Morning Report*: "While we may not have agreed on many tort policy issues, John was always a gentleman and worthy opponent."

A journalism graduate and a lawyer, Sullivan was an articulate spokesman for common-sense legal reform. In an article he contributed in 2006 to the magazine of the PIAA, the national organization for medical professional liability companies, Sullivan likened excessive litigation to biological disease, describing it as having "an ability to mutate to cope with stronger defenses or benefit from new opportunities." Those new opportunities were what Sullivan's tenure at CJAC fought to defeat.

As noted in the *Sacramento Bee*, Sullivan commented on his retirement from CJAC: "When we began in 1995, we were barely even recognized in the Legislature. We had a substantial [appellate court] program and we didn't have too much else. But since then, we've built a highly respected legislation operation . . . and we've gotten into political campaigns in a very winning way." Under the leadership of CJAC's current president, Kim Stone, the organization's robust voice endures.

CAP is represented on CJAC's Board of Directors.

Case of the Month

by Gordon Ownby

Don't Rely Simply on Tidy Phrases in Your Chart

Just as the law does not require a physician to deliver a mini-course in medicine when discussing options and risks with a patient, juries will not expect that every nuance of the original event will be captured on the charted page.

But electronic chart narratives containing standard, generalized phraseology will bear poor witness in a subsequent dispute over medical care.

A 91-year-old woman visited Dr. OS, an orthopedic surgeon, after suffering a left femoral neck fracture in a fall. Dr. OS recommended a hemiarthroplasty and discussed the risks, benefits, and alternatives with the patient. The surgery was uneventful and the woman was discharged to a skilled nursing facility (SNF) for rehabilitation.

Nursing notes indicate that 12 days into her tenure at the SNF, the patient had increased confusion and that the surgical incision showed signs of infection, serosanguinous fluid, and some bleeding. When Dr. OS was called with this information, he ordered a seven-day regimen of Keflex.

Lab results showing increasing white blood cell counts were reported to the patient's attending physician and a urine test showed E. coli. A culture taken from the patient's hip incision six days after the Keflex order showed staphylococcus aureus. During that period, the patient became more disoriented and complained of increased pain, though there is no indication that Dr. OS was so advised.

The patient and her son visited Dr. OS for the three-week post-op evaluation the day the incision culture was taken. Though Dr. OS' formatted, typed report shows that the son reported his mother had persistent delirium and was diagnosed with a urinary tract infection, the signed document makes no mention of the Keflex order. Other passages were light on detail, including:

"Past medical history, family history, social history, and review of symptoms were reviewed with the patient and documented in the chart with no changes from the previous visit."
"Joints, bones, and muscles: Her surgical incision is healing well and no erythema or drainage."

"I personally reviewed with the patient the radiographs of the left hip from the skilled nursing facility. This demonstrates well-positioned hip hemiarthroplasty with no sign of implant complication or loosening."

"I had a lengthy discussion with [the patient] regarding the natural history of this condition, the multiple treatment options, and the risks and morbidity of the various treatment options and the condition itself."

At that visit, Dr. OS wrote that he will see the patient back in four weeks with repeat radiographs and that he will order the staples be replaced with Steri-Strips.

The next morning, the staff at the SNF attempted to remove the staples but encountered heavy drainage. Nursing staff calls early that afternoon were unsuccessful in reaching Dr. OS. A nurse at the office offered the opportunity to speak to another orthopedic surgeon but otherwise recommended contacting the patient's attending physician. The patient was admitted to the hospital that evening with purulent drainage from the incision. Her condition deteriorated rapidly and she died two days later. The death certificate listed sepsis of the left femoral fracture as a significant contributor to the patient's death.

In the family's claim against Dr. OS, the son insisted that in the post-op visit, his mother was in pain and that Dr. OS never looked at the surgical incision. The family resolved the dispute with Dr. OS prior to litigation.

A patient's or a family's account of their medical experiences will often include a vivid description of events. Without a chart that offers its own key details of what actually transpired, prevailing in any ensuing credibility contest will be difficult.

Gordon Ownby is CAP's General Counsel. Comments on Case of the Month may be directed to gownby@CAPphysicians.com.

Service Animals in the Medical Office

by Kimberly Danebrock, RN, JD

Service animals are essential to many individuals with disabilities. Under the federal Americans with Disabilities Act (ADA) and California law, a service animal is a dog that has been individually trained to do work or perform tasks for an individual with a disability. Further, the specific task performed by the dog must be directly related to the person's disability.

Dogs can be trained to assist the disabled with the activities of daily living and to provide safety by being trained to guide the blind, alert the deaf, protect a person having a seizure, assist a person in a wheelchair, and alert diabetics that their blood sugar is dangerously low or high.

Although a service animal must be a dog, the dog can be any breed. The dog does not need to be professionally trained, be certified, or wear anything that identifies it as a service animal. The handler is responsible for care and control of the dog. If the dog is out of control and the handler does not take action, the office staff can request the animal be removed from the office.

Medical offices must make reasonable efforts to accommodate individuals with disabilities by allowing service animals into the office. However, sometimes it is not obvious that the dog is a service animal. In order to avoid unlawful and discriminatory treatment of those with disabilities, office staff may only ask two specific questions: (1) is the dog a service animal required because of a disability? And, (2) what work or task has the dog been trained to perform? Office staff may not request documentation for the dog, require that the dog demonstrate its task, or ask about the nature of the individual's disability.

Psychiatric Service Dogs and emotional support dogs are treated differently under the ADA and California law. Psychiatric service dogs are trained to recognize and respond to an individual's need for help. They perform trained tasks that are directly related to the individual's psychiatric disability. A psychiatric service dog may be trained to interrupt destructive behavior or remind an individual to take his or her medication.

In contrast, a dog that provides an individual with emotional comfort or a sense of safety, but is not specifically trained to perform a task directly related to the individual's psychiatric disability, is an emotional support dog. Because they have not been trained to perform a specific job or task, they do not qualify as service animals.

Service dogs play a vital role in assisting disabled individuals to participate in life more independently. For more information about the ADA, visit www.ADA.gov or call the ADA Information Line at 800-514-0301 or 800-514-0383.

Kimberly Danebrock is a Senior Risk Management and Patient Safety Specialist for CAP. Questions or comments related to this article should be addressed to kdanebrock@CAPphysicians.com.

COOPERATIVE OF AMERICAN PHYSICIANS

Cooperative of American Physicians, Inc.
333 S. Hope St., 8th Floor
Los Angeles, CA 90071

PRESORTED
STANDARD
US POSTAGE PAID
LOS ANGELES, CA
PERMIT #1831

March 2016

IN THIS ISSUE

CAPsules® is a publication of the Corporate Communications Department of the Cooperative of American Physicians, Inc.
333 S. Hope St., 8th Floor, Los Angeles, CA 90071 | 800-252-7706 | www.CAPphysicians.com

We welcome your comments! Please submit to communications@CAPphysicians.com