Hawkeye Highlights

Iowa AAHAM Chapter

Photo By: Steph Hultman

Summer 2017

Volume 9, Issue 2

Message from the President.....

Rebecca Gough
President, Iowa AAHAM

Greetings, Fellow Travelers!

The first six months of my term as your chapter president have been very busy, as well as educational. Now that I've attended 3 National Board meetings I'm more impressed with this organization than ever.

We often hear, "Do something today that your future self will thank you for." Being a member of AAHAM is a great "something" that you do for yourself, for your career, and for the future of your community. In the challenging and changing world of healthcare financing AAHAM provides many ways to stay informed and even to help shape national policies.

Legislative Day was an opportunity to meet directly with Senators Ernst and Grassley and with advisors to Representatives King and Blum. More about these meetings elsewhere in this newsletter.

The National Board has made available for the first time free student memberships. Any college student taking 12 semester hours is eligible to be a National Member. This opens the door for a student to learn directly from those of us involved in the day to day work of healthcare finances. So many of us "old-timers" grew up in the field and have had to learn as we went along. I remember my mentor from the late 1970's. She was very thorough in her work and helped me learn health insurance from the ground-up. Now almost 40 years later I hope that I have imparted some wisdom along the way to the next generation.

Your involvement with AAHAM is so important in so many ways. In September we will hold elections for at least 3 board positions. I encourage everyone to consider submitting your name for nomination. Your future self will thank you for taking that first step to new challenges.

Your future begins now! ▲

Respectfully,

Rebecca Gough

Table of Contents

Summer 2017

For Corporate Sponsor Program inquiries, contact:

Ashley Allers, Corporate Sponsorship Chair
Van Diest Medical Center
2350 Hospital Drive
Webster City, IA 50595
Phone: (515) 832-7705
Email: AAllers@vandiestmc.org

For membership information, or to submit changes of address, contact:

Stephanie Hultman, Membership Chair
Craneware
1126 Linbud Lane
Waterloo, IA 50701
Phone: (319) 240-5306
Email: sjhultman@mediacombb.net

For questions and comments regarding** Hawkeye Highlights, **contact:

Stephanie Hultman, Publisher
Craneware
1126 Linbud Lane
Waterloo, IA 50701
Phone: (319) 240-5306
Email: sjhultman@mediacombb.net

Laurie Gaffney, Editor
Buena Vista Regional Medical Center
1525 West Fifth Street
Storm Lake, IA 50588
Phone: (712) 213-8678
Email: gaffney.laurie@bvrmc.org

Hawkeye Chapter

Officers - Board Members - Committee Chairs

Rebecca Gough	*President*
Connie Dudding	*Vice President / Program Chair*
Audra Ford	*Secretary / Registration*
Becky David	*Treasurer / Nominating Chair*
Cristie Knudsen	*Chairperson of the Board*
Jack Stanton	*Board Member / Website Chair*
Bobbie Jo Harrings	*Board Member / Hospitality Chair*
Stephanie Hultman	*Board Member / Newsletter / Membership Chair*
Ashley Allers	*Board Member / Corporate Sponsorship Chair*
Connie Dudding	*Legislative Chair*
Sarah Sumpter	*Certification Chair*
Laurie Gaffney	*Newsletter Editor*

HAWKEYE HIGHLIGHTS EDITORIAL POLICY & OBJECTIVES

The HAWKEYE HIGHLIGHTS newsletter is published four times annually by the AAHAM IOWA CHAPTER to update the membership regarding chapter and national activities as well as to provide information useful to health care administrative professionals. Opinions expressed in articles or features are those of the author(s) and do not necessarily reflect the views of the Iowa Chapter. AAHAM, the NATIONAL AAHAM organization or the editor. Reproduction and/or use of the format or content of this publication without the expressed permission of the author(s) or the editor are prohibited. ▲

2017 AAHAM Annual National Institute (ANI)

Scholarships AVAILABLE

Submitt your Applications in NOW .....

The 2017 Annual National Institute will be held at the Opryland Resort in Nashville, TN from October 18-20, 2017.

Put the date and location in your Outlook Calendar now! The Hawkeye Chapter of AAHAM is sponsoring **2 scholarships** to the Annual National Institute (ANI), to be held at the Opryland Resort in Nashville, TN. The scholarships will cover registration, plus $300 towards travel/hotel expenses. The scholarships will be awarded based on points earned between July 1st and June 30th. Members can earn points in a variety of ways:

- 1 Point earned: Every article referred to and published in the Hawkeye Highlights
  Every new member referred (as documented by National)
- 2 Points earned: Every article authored and published in the Hawkeye Highlights (not including required committee reports), Membership on a committee of the board, as verified by the committee chair
- 3 Points earned: Every meeting attended (e.g. Spring Meeting, Fall Meeting, educational meetings sponsored or cosponsored by the Hawkeye chapter).

Points will be tabulated for members that apply and in the event of a tie; a random drawing will be held. Winners will be selected around August 1st and will be notified by August 15th. The Board is excited to be able to offer this opportunity to members.

The ANI always offers informative, timely educational sessions. And the networking opportunities are limitless. So, start reading those industry magazines and refer those articles. Or, get out your pen and author an article on the topic nearest and dearest to your heart. Better yet, attend the Spring Conference in May or one of the joint educational conferences coming up and you may find yourself already on your way to Nashville! ▲

See the Scholarship Program rules on the next page.

Hawkeye AAHAM Chapter Scholarship Program

Eligibility:

- Local Hawkeye Chapter member for at least 1 year:
- If not a National member, recipient will be responsible for national dues;
- The President & Chair of the Board are ineligible;
- Points are accumulated for the 12 month period beginning July 1st and ending the following June 30th

1 Point	2 Points	3 Points
■ Every article referred & published in Hawkeye Highlights ■ Every new member referred	■ Every article authored & published in Hawkeye Highlights ■ Membership on a committee of the board	■ Every AAHAM sponsored meeting attended

Name:_____ AAHAM ID # _____

Address: _____

E-Mail: _____ Telephone: _____

Signature: _____ Date: _____

Date	Activity	Points	Verification*

** To be completed by the AAHAM Board*

Please submit completed application by July 15th to:

- Stephanie Hultman - sjhultman@mediacombb.net

Certification – I Passed! Now What?

Submitted By: Sarah Sumpter, CRCS-I/P, CRCR

You have studied for hours until your eyes watered from reviewing the book or a stack of flashcards. The day arrives and you take your test. You Passed! After the initial joy dissipates, you start to think, now what do I need to do.

One answer is to retest every three years to maintain the certification. But let's be honest, it is a lot of work and most people would prefer not to retest. Luckily, AAHAM provides us with an option to accumulate Continuing Education Units (CEU's). To get started, join National AAHAM if not a member already. CEU's only begin to accumulate starting as of the join date as a National AAHAM member.

The number of CEU's required to maintain each type of certification is available at http://www.aaham.org/Certification.aspx under the Recertification tab.

CEU's can be obtained a number of ways including but not limited to authoring articles, attending AAHAM events, serving on the AAHAM board, and proctoring certification tests. Previously these CEU's were reported on a paper form with attached documentation. Based on previous suggestions and to move forward with technology and ecology, National AAHAM has switched to an online CEU reporting form. The online reporting form is located here: http://www.aaham.org/Certification/RecertForm.aspx. This form also allows attaching scanned copies of supporting documentation as required to substantiate the CEU activity. Members can also use the CEU database on AAHAM.org to track the ongoing number of CEU's accumulated.

AAHAM certification helps individuals and teams expand and sustain their knowledge of the revenue cycle. In using the continuous education process, one can stay up to date on important changes and updates in the healthcare environment. The activities that contribute to obtaining CEU's promote further professional development and personal growth.

Visit AAHAM.org today and find out what certification is the next rung on your ladder to career success! ▲

2017 Certification Schedule

CRCS-I and CRCS-P

August 15, 2017
Registration deadline for November 2017 Exam Period

November 6-17, 2017
November 2017 Exam Period

December 15, 2017
Registration deadline for March 2018 Exam Period

2017 AAHAM Fall Conference Agenda

September 14-15, 2017
Hilton Garden Inn - Johnston, IA

Thursday, September 14th, 2017

Improving First Pass Denial Rate: Why Aren't My Days in the 30s?
Sue York, Director of Operations, OS Inc, RHIA, CPC, COC

Long gone are the days when the benchmark for superior performing hospitals was somewhere under 60 Gross Days Revenue Outstanding (GDRO). With payment turnaround for most major payers averaging 15 days, providers who submit a high volume of clean claims will see GDRO in the 30's.

No Experience Required: Building Your Best Business Office Team
Sue York, Director of Operations, OS Inc, RHIA, CPC, COC

Build a winning team in your business office by hiring, developing and retaining talented individuals – and by making a clean break with those staff who are culture killers.

Hiring – Explore the approach of hiring for characteristics over experience to find your ideal talent using these specific interview techniques and skills assessments.

Training & Staff Development – Understand how to best train your staff on each function of the business office: Registration, Billing, Denials, Follow-up, Collection and Customer Service. You will receive everything you need to implement your own business office training program, from an outline of our Insurance 101 training to samples of procedures, quizzes, job descriptions, evaluations and more.

Retention and Firing – Learn how to reward your "super stars" and keep them engaged as well as how to identify and break ties with the staff who are not contributing to your organization's goals.

VA Claims Program – *Tony Taylor, Benefits Recovery*

Wellmark - *Nicky Cooney*

Amerigroup - *John Hedgecoth and Sarlynn Heston*

Friday, September 15th, 2017

IHA – *Ericka Eckley*

UnitedHealthcare – *Megan Cavanagh and Sheryl Houk*

AmeriHealth – *Tim Rau*

WPS Medicare – *Aileen Sigler*

AAHAM Legislative Day

American Association of Healthcare Administrative Management

Submitted By: Rebecca Gough

May 1st and 2nd was a time for AAHAM members to discuss and learn about national policies that are before Congress that affect our jobs as well as our personal lives. Few, if any of us, escape the use of the healthcare system in our lifetime.

Representative Joe Courtney, D-CT introduced legislative bill H.R. 1421 to amend the requirement for a 3-day acute care stay in order to qualify for SNF care. Representative Courtney spoke at our morning session explaining his reasons for introducing this bill and how the requirement has affected his family. Senator Sherrod Brown, D-OH is the sponsor of S.568 in the Senate.

2017 AAHAM Legislative Day. Bill Carlson, Mike Dobbs, Senator Charles Grassley and Rebecca Gough.

In 2016, AAHAM joined a consortium of 29 stakeholders in support of such legislation and since then has participated in written and verbal communications with members of congress as well as Health and Human Services (HHS). In July, 2013, the Office of the Inspector General reported that in calendar year 2012 beneficiaries had 617,702 hospital stays that lasted at least three nights, but that did not include three inpatient nights. The report was supportive of counting observation days towards the 3-day inpatient stay minimum required. (https://oig.hhs.gov/oei-02-15-00020.pdf) What we got instead was the 2-midnight rule which did not resolve the problem.

The official position of AAHAM is on the National Website. What is often discussed and used as examples to support this position is patients who have been in observation status at a hospital for several days, sometimes as long as 13 days. When they are then discharged to transfer to skilled care, they find out the skilled care won't be covered since their status was not that of an inpatient. These are the cases that have received national attention.

My personal opinion is that the opposite is more common. A person comes into the hospital through the emergency department or as a direct admit from a physician's office. They are recognized as an outpatient in the facility. During the next 24-48 hours they are evaluated and observed and deemed to be a candidate for skilled care. Moving them to a skilled level of care would allow the patient to be served in an appropriate level of care without having to be an inpatient for 3 days to meet the Medicare requirement.

Continued on Page 8 . . .

Continued on Page 10 . . .

2017 AAHAM Legislative Day. Rebecca Gough, Senator Jody Ernest, Mike Dobbs and Bill Carlson.

Meeting with Senators Ernst and Grassley and staff of Representatives King and Blum was an opportunity to present both scenarios and the consequences to Medicare beneficiaries. Both Senators have signed on in support of S.568.

I thank you as members of the Iowa Hawkeye Chapter to allow me to participate in this grassroots effort on your behalf. I also thank Mike Dobbs and Bill Carlson for their input and experience. This experience is another opportunity available to all AAHAM members. Join us next year. If the bills pass this session, we will have a new topic to present.

Hawkeye Chapter of AAHAM

Balance Sheet

Treasurers Report for Period
Ending: 12/31/16

ASSETS:	
Cash in Bank	$14,684.88
Certificate of Deposit *#30063596*	$6,093.07
Certificate of Deposit *#30063430*	$3,237.53
TOTAL ASSETS	**$24,015.48**
LIABILITIES:	
Payables	$0.00
EQUITY:	
TOTAL LIABILITIES AND EQUITY	**$24,015.48**

Operating Statement

REVENUES:	
Corporate Sponsor Fees	$ 3,749.10
Technical Exams	$ 3,714.68
Registrations/Spring 2016	$ 8,058.33
Registrations/Fall 2016	$ 5,319.18
Donations	- - -
Other Revenue	$ 755.00
TOTAL REVENUE	**$21,596.29**
EXPENSES:	
Travel	- - -
Website	$ 1,174.00
Insurance Fees	$ 1,182.00
Spring Conference 2016 Speaker Fees	$ 5,444.33
Spring Conference 2016 Facility/Hospitality Fees	$ 1,351.55
Misc.	$ 10.00
AAHAM National Legislative Day 2016	$ 269.00
Fall Conference 2016 Speaker Fees	$1,261.08
Fall Conference 2016 Hotel Fees	$4,101.87
Fall Conference 2016 Hospitality	$ 318.02
Fall Conference 2016	$ 9.54
AAHAM Legislative Day 2016	$ 269.00
ANI Expenses	$3,913.57
TOTAL EXPENSES	**$ 19,034.96**
NET INCOME (LOSS)	**$2,561.33**
BEGINNING CASH BALANCE	**$12,243.55**
ENDING CASH BALANCE	**$14,804.88**

Respectfully,

Becky David

Chapter Treasurer

AAHAM Board Minutes . . .

February 1, 2017
3:00 pm

I. Roll Call

Cristie, Rebecca, Connie, Becky, Bobbie, Steph, Jack, Ashley, Melissa, Sarah, and Audra

II. Secretary's Report

Connie emailed out minutes from September meeting. They were approved electronically.

III. Treasurer's Report

Becky reported as of 10/31/16 bank checking account totaled $14,684.88 and 2 CD's totaling $9319.35

IV. Committee Reports

a) Website. Jack volunteer to chair as Becky was elected as Treasurer. Becky will send him contact info.
b) Newsletter. These are published in March, June, September and December. They are always looking for more information to include. Laurie will reach out for information a month prior to publication.
c) Membership. Rebecca sent out emails to 26 non-renewing members. A total of 83 members to date. Student membership is free if anyone knows of students looking to join.
d) Corporate Sponsor. Ashley volunteered to chair as Melissa is no longer on the board.
e) Legislative Day. Registration is now open. This takes place on May 1st and 2nd. Becky moved and Steph 2nd for the Chapter to pay to send 2 representatives. Motion carried. Rebecca will be attending and looking for another volunteer to go with her. Hotel is $295 per night. Subjects to be discussed are the Observation Two-Midnight rule, the Moon, and TCPA.
f) Certification. Sarah reported that 32 passed certifications in November. We should be expecting a deposit of $420 coming soon. The largest organizations represented are Avadyne and Unity Point. There are 37 signed up for the CRCS and 1 for the CRCE in March. It has been discussed to have the I and P exams together but no action yet. Rebecca heard that they are now offering online webinars to study but has been unable to find them. If found we will show at the May meeting.

V. ANI 10/18-10/20/17

Early Bird Registration is due 2/28/17-$150 savings-held at Opryland Resort

a) The chapter gets one free registration and will send Rebecca.
b) Discussion was held around continuing to offer scholarship to send additional members. It was decided to continue with the same point system. Steph will publish this in the newsletter.

VI. Old Business

a) Awards. Tara has 40 year award as well as several paper awards. What should be done with them? Nothing decided.
b) Projector. Currently we depend on Luke or Rebecca to bring to meetings. Steph will get pricing for the purchase of projector and clicker. Moved by Becky and 2nd by Ashley to approve purchase of new machine with $700 limit. Motion carried. This will be stored by the Vice-President.

Continued on Page 11 . . .

. . . Continued from Page 10

VII. New Business

a) Bylaws. Rebecca has been put on the national Policies and Standards committee. They were last updated on 2/4/08. Rebecca will research who is responsible to keep these updated and will reach out for assistance in updating them.

b) Payor Panel. Steph asked if our AAHAM chapter would like to be a co-sponsor of this meeting. This would mean sharing in the profits and expenses. The Fall meeting had 112 registered for $4200. Expenses were $2000 ($1700 in catering, $250 for WPS, and $50 for online registrations). We ask that they agree not to have in months surrounding our AAHAM meetings since we typically have the same offering. Payor Panels usually held in March and November. Board will be responsible to help with registration and introduce speakers. This will give us the opportunity to advertise our meeting and certifications.

c) Spring AAHAM Meeting
   i. May 18-19th
   ii. Offer Vendor "Speed Dating?" Do this before lunch and offer it as a sponsor perk.
   iii. Hot Topics-Moon, Non-emergent ER MCO reimbursement, Map Apps-See if Sara McClure at Henry County will share about what they did to win award.

VIII. Meeting adjourned

4:15 PM – Connie and Audra ▲

Respectfully,

Audra Ford

Website Alert

The Iowa Hawkeye Chapter is excited to announce our website for members at www.hawkeyeaaham.org. The site includes:

Chapter officers and board members
Upcoming events-Calendar of events
Chapter Bylaws
Sponsor Information
Membership information
Link to the National AAHAM Website
Current and Past Newsletters
Photos from past meetings

Watch for more information to be added every month. Since the site is new, we are looking for any ideas for additional information from our members. Please contact board member Jack Stanton at jacks@thehaugegroup.com with ideas. ▲

Get a *Clue*! Eliminate All Timely Filing Adjustments

Written By: *Peter Angerhofer, Principal at Colburn Hill Group*

In the popular board game *Clue*, players move about the board collecting information about a murder. As they find out what didn't happen – it wasn't Miss Scarlet, it wasn't with the rope, it wasn't in the Billiard Room – the winner eventually narrows it down to the only possibility: Professor Plum in the Conservatory with the Candlestick! (It isn't always in the Conservatory, but it somehow is ALWAYS Professor Plum!)

The game works because players can differentiate between the various locations, suspects, and weapons. It wouldn't work if every clue was the lead pipe.

Unfortunately, too many PFS shops treat their write offs like a bad game of *Clue*. When they find claims that are too old to bill, or when they perform regular cleanups of aged or low balance AR, they use adjustment codes like "Exceeds Filing Limits." In the process, they lose data that might otherwise give them insight and allow them to catch that dastardly Professor.

It is an unfortunate fact of running a revenue cycle that many claims will "die" of old age. Most often, the limit that is exceeded is actually an appeal limit triggered by multiple appeals which eventually exceed the deadline for appeal or a missed appeal window (60 or 90 days.) In a few cases, a bill will be held in the editor or at a clearinghouse past a filing limit. It is extremely rare that a bill simply sits in DNFB too long and once billed is denied simply because it was overlooked, forgotten, or somehow slipped through the cracks. In short, the vast majority of claims that deny for exceeding filing limits have *some other problem which caused the delay in billing*. Calling the write off a Timely Filing Adjustment not only fails to provide any insight into the upstream causes, it actually masks the real problem.

If your adjustment codes say everything looks like a lead pipe, it is awfully hard to know that it was really the candlestick, and if you don't know it was the candlestick, then it is harder to look for the right clues to who murdered the beautiful, innocent claim which now lies at your feet. In applied terms, if everything looks like a timely filing write-off, it appears that the problem is in billing and follow up. But unless something is seriously broken in PFS, the strong likelihood is that those timely filing write-offs are really a mix of authorization, medical necessity, billing error, and other denials. If, for example, most of your authorization denials are being buried in timely filing, you may not realize that authorizations are a problem: "*The auth write-off is small, so patient access must be doing its thing – these darn payer limitations are the real problem*."

But if those auth problems were broken out and categorized appropriately, the picture might be very different. It would be easy to identify the lack of authorizations as the root cause of the problem. **The answer is to eliminate all use of (or nearly all) Timely Filing write-off codes**.

The conceptual solution in *Clue* is pretty simple – all the suspects and all the potential weapons are right there – just figure out which one is the murderer! A clear goal, but it takes some effort to achieve. Similarly, the conceptual approach of eliminating all Timely Filing adjustments seems simple, but it actuality it requires work to follow the clues and accomplish the task.

In some cases, posting logic is set to automatically adjust any Timely Filing denial. (In the worst case scenarios, those adjustments go to Contractuals rather than Denials. In those cases, all visibility into the size or shape of the denial problem is lost!) While this might seem like a time saver – *if the claim is past limits, the revenue is lost so why should we spend any time on it?* – but there really are two potential losses:

Continued on Page 3 . . .

. . . Continued from Page 12

First, the timely filing denials might not be legitimate. Perhaps a bill was sent or an appeal was filed but the payer didn't appropriately load it into their system. Or perhaps the bill was delayed for some legitimate reason that might lead a payer to make an exception. So a claim that could be recovered instead is declared dead.

Second, even if the revenue is truly lost, it is likely the mistake will be repeated unless you can learn from this failure. Whether it is sizing the scale of the problem or localizing it by department or payer, appropriately maintained data is a key driver of improved performance. This is essential to keep recoverable claims alive in the future!

Revising the posting logic is a relatively easy step, but the next step is more challenging – if you haven't auto adjusted the claims but they still need to be written off the AR, then someone has to take the time to make the adjustment. The inclination from staff will likely be to look at the last denial and use that as the adjustment code – denied for Timely Filing, written off to timely filing – but doing that will only repeat the same error, just at greater expense.

Staff need to spend some time researching the claim (and need to be trained that expending the time is appropriate) to understand what caused the claim to deny in the first place, and using THAT adjustment code. It is more work and will take more time, but having an accurate reflection of the problems causing adjustments is vital to solving the problems. Even a careful AR manager may be surprised by how the distribution of adjustments changes when timely filing claims are re-distributed to more discrete, meaningful adjustment categories. And that AR manager may enjoy the side benefit of making themselves look good as adjustments shift from the PFS focused Timely Filing Codes to other codes that may be Patient Access or Coding related!

Encouraging staff to move away from the use of timely filing may be difficult – their training and years of experience have likely built a strong tie between the last denial code and the adjustment reason – but there is one way to make a clean break: **Eliminate the Timely Filing adjustment codes**.

There are very few legitimate uses of the codes to begin with, when they are used they tend to mask the real problem, and staff tend to over- (or mis-) use them. It may mean there are a handful of claims that don't have an appropriate home, but the other benefits far outweigh this potential, minor cost.

Claims are going to die, for a variety of reasons, and the obvious cause of death might be a timely filing denial. But PFS managers should look beyond the obvious and take into account the root causes of those losses, which rarely are solely because of filing limits. Understanding root causes is an extremely valuable clue, which can lead to better understanding of adjustments, reduced write-offs, and ultimately increased collections.

Not to mention finally bringing Professor Plum to justice. ▲

Peter Angerhofer is a principal at Colburn Hill Group [www.colburnhill.com.](http://www.colburnhill.com) CHG brings deep experience in operations to Revenue Cycle improvements; we treat the root causes, not the symptoms, of Rev Cycle challenges through our operational-level knowledge and tech-enabled solutions.

Corporate Sponsors

The Iowa Hawkeye Chapter wishes to thank its Corporate Sponsors. Their generous financial contributions help ensure our chapter meets its goals and objectives, and allow us to provide educational programs, social functions, training programs for member certification, and the Hawkeye Highlights newsletter.

Platinum	**Avadyne Health** **The Hauge Group**
Gold	**Eagle Recovery Associates**
Silver	**AAMS**
Bronze	**MaxRTE** **Tri-State Adjustments, Inc.** **Bloom Payment**

Certification Passed Exams – CRCS-I, P

Submitted By: Sarah Sumpter, CRCS-I/P, CRCR

Congratulations to the following people on their recent certification testing! These folks were successful in obtaining their CRCPS-I, P Certification. The exams were taken this past March - Congratulations on a job well done!!

Passed CRCS-I Exam in March		Passed CRCS-P Exam in March	
Kathy Henrichs	UnityPoint Health - DMS	Alicia Garland	Avadyne Health
Katherine Mclahlan	UnityPoint Health - DMS	Shawna Harrah	Avadyne Health
Diane Moller	Mercy Medical Center	Erin Keller	Avadyne Health
Marti Muchler	UnityPoint Health - DMS	Lynne Klemp	Avadyne Health
Laura Nunez	UnityPoint Health - DMS	Renee Munden	UnityPoint Health - DMS
Joseph Rude	Avadyne Health	Billie Norby	Avadyne Health
Lavonne Seaton	Avadyne Health	Kim Stainbrook	Avadyne Health
Christine Taylor	Avadyne Health	Sarah Vaux	Avadyne Health
Shawn Vanderpool	Avadyne Health		

Cybersecurity—Protecting Your Organization

Written and Submitted By: ProAssurance

With increased use of technology comes increased risk of cyber-attacks. Anything transmitted or stored electronically is at risk of being stolen.

Many people don't think that—or understand why—medical information is valuable or at risk. A compilation of 2014 reported data-breach statistics reveals there were 783 security breaches in the United States. Of those, 42.5% were breaches of medical or healthcare information. This includes over eight million individual healthcare records accessed or stolen through cyber-attacks.[1]

Large healthcare systems, hospital networks, and individual healthcare providers have all been attacked; however, the size of an entity is no clear indication of the size of the breach. For example, one Blue Cross Blue Shield attack yielded only 300 records, while a large Tennessee system's breach yielded approximately 4.5 million records. Several individual physician practices were breached as well, yielding as many as 7,500 records from one practice.[2]

Why are medical records targeted?

Medical records are likely targeted because they contain all of an individual's personal information: finances, social security number, health information, and family information. This gives thieves more potential uses for stolen information, including applying for credit cards, store accounts, or other lines of credit. Thieves also can use the information to steal healthcare services or fraudulently bill healthcare insurance providers and Medicare/Medicaid.

Victims may not discover information theft for several months—or even years. In some instances, victims have received debt collection efforts for medical services they never received. These are just a few reasons why a medical record can fetch up to $50 on the black market, while a credit card number may only earn $5.[3]

Another example of how valuable a medical record may be: a security firm CEO shared an example of a black market advertisement to sell ten Medicare numbers: "It costs 22 bitcoin—about $4,700 according to today's exchange rate."[4]

The transition to electronic health records has given criminal hackers more opportunities to steal medical records. The chief information officer for a hospital system in Salt Lake City states his hospital system "fends off thousands of attempts to penetrate our network each week."[5]

Ease of access also is a factor. Some hospitals and healthcare providers are using systems that have not been updated in more than ten years.[6] While organizations rush to prepare for ICD-10 implementation and meaningful use, cybersecurity may be falling through the cracks. Many healthcare systems "do not encrypt data within their own networks."[7] Once a hacker penetrates whatever security the system does have, the unencrypted information is there for the taking.

Electronic medical devices offer a way in

Cyber criminals sometimes use medical devices to access a hospital's or facility's network. Medical devices rarely contain the information criminals are looking for; however, they can use these devices as an "entry and pivot point in the network."[8]

When cyber criminals break into a network, they can access virtually any information the facility has stored electronically. Not only do they target patient records, cyber criminals have been known to target research data, trigger system malfunctions, or deploy ransomware. Ransomware is a type of software that holds electronic information hostage until the owner pays a ransom to get it back (much like a kidnapping).[9]

Continued on Page 16 . . .

. . . Continued from Page 15

A recent example is a hospital that discovered three blood-gas analyzers infected with malware. The devices contained a "firewall, heuristics-based intrusion detection, endpoint security, and antivirus tools—as well as an experienced security team."[10] The firewalls and security were purportedly managed by the manufacturer's IT security team.[11] It's not uncommon for device manufacturers to prohibit a hospital's IT security team access to the internal network of the devices they sell.

Not only do medical devices potentially offer access to a hospital's network; hackers also could manipulate and affect patient care. A recent article points out the possibility that a hacker could "gain control of the devices remotely and … instruct an infusion pump to overdose a patient with drugs, or forc[e] a heart implant to deliver a deadly jolt of electricity."[12] The Department of Homeland Security (DHS) is currently reviewing infusion pumps and implantable heart devices for potential security issues.

Another example of cybercrime is hospital data "being siphoned out and sent to a location in Guiyang, China."[13] This resulted from a hospital employee inadvertently downloading a malware infection by visiting a malicious website. This provided the attackers remote access to the network, which they used to insert a backdoor on the hospital's picture archive and communications system (PACS).[14]

Lessons learned from a DDoS attack

DDoS stands for distributed denial-of-service. These cyber-attacks infiltrate computer networks with the sole purpose of disrupting normal business operations and creating havoc. Hackers who initiate these attacks often justify their actions as social activism. Examples include: preventing patients from accessing a hospital's website, keeping clinical staff from sending and receiving emails, disrupting eprescribing systems, or general disruption of a hospital's network.

Boston Children's Hospital fell victim to a DDoS attack in March and April of 2014. The hospital received advanced warning and immediately convened their incident response team. They also employed a third-party IT team. At the peak of continuous attacks, the hospital "took down all websites and shut down email, telling staff in person that email had been compromised. Staff communicated using a secure text messaging application the hospital had recently deployed."[15] Fortunately, the hospital's internal networks (such as its EHR) remained uncompromised.

The attack was reportedly initiated by a hacker group known only as "Anonymous." The group was acting in "response to the hospital's diagnosis and treatment of a 15-year-old girl removed from her parent's care by the [state]."[16] The hospital was able to avoid significant damage and disruption by being proactive and taking the threat seriously.

The hospital's CIO and Senior VP for Information Services identified **six lessons learned**:

1. Develop DDoS countermeasures;
2. Be familiar with your electronic systems and know which ones depend on external internet access;
3. Have an alternative to replace email communications;
4. When dealing with a security threat, push security initiatives and don't make excuses (the hospital shut down email communications, eprescribing, and external-facing websites);
5. Secure teleconferences; and
6. "Separate signals from noise." Amid the Anonymous attack, several staff members reported strange phone calls from a number listed as 000-000-0000. At the time, it was hard to tell if this was related, and it made the whole incident that much harder to manage. [17]

Email can be risky

Phishing emails are popular with hackers and other cyber attackers. These emails typically prompt the recipient to

Continued on Page 17 . . .

. . . Continued from Page 16

click on a link to access purportedly important information. When the recipient opens the hyperlink or the email itself, the hacker gains access to the computer. Once in, they can install malicious software, steal information, or access the network the computer is attached to.

So, what does a phishing email look like? They typically include:

- Poor grammar;
- misspellings;
- Threats—such as stating your information has been stolen and providing a link to file a report;
- Hyperlinks that appear to link to a trusted site, but actually redirect you elsewhere (check the address by hovering your mouse over the hyperlink to reveal the actual web address); and
- Recognized logos and design that mimic legitimate businesses.[18]

What can you do to safeguard your network?

When implementing or updating an EHR system or purchasing a medical device, talk to the vendor about cybersecurity. Ask whether the stored information is encrypted. It also is a good idea to determine if or when the vendor will provide security updates.

Organizations may need to "invest more money and employee talent in shoring up the walls around their electronic data."[19] Cybersecurity is a highly specialized area that requires expertise. Your EHR vendor may be able to provide some assistance in this area, but remember their expertise is creation and functionality. Hiring in-house cybersecurity experts or contracting with a cybersecurity firm specializing in this area may be best to protect your organization and your patients.

Several organizations offer guidance and resources on cybersecurity, including: Department of Homeland Security, American Hospital Association, Centers for Medicare & Medicaid Services, and National Institute of Standards and Technology (NIST). Their web addresses are included in the endnotes of this article.[20] These are just a few of many resources available to assist with cybersecurity.

Specifically, NIST has developed a "Framework for improving critical infrastructure cybersecurity." Healthcare is considered part of the critical infrastructure of the United States; therefore, the "framework" is intended for hospitals and other healthcare facilities. It provides "global standards, guidelines, and practices to enable critical infrastructure providers to achieve resilience."[21] While the framework is currently a voluntary guide, some argue it should become mandatory. You can access it online at NIST.gov.

Tips to Reduce Risk:

- **Be proactive**—Chances are good that your facility will face a cyber attack within the next five-to-ten years. Implement cybersecurity to make it tougher for hackers to access your network. Review the National Institute of Standards and Technology[21] framework to help determine whether your cybersecurity is sufficient.
- **Have a plan**—The most important tool in your cybersecurity tool box is a plan of action that covers all aspects of your facility's network (not just your EHR and website).
- **Train**—Ensure all staff know what to do if they suspect a cyber breach has occurred, including: who to contact, their roles, and all steps for which they are responsible. Educate staff about how to identify malicious or phishing emails. Consider activating your incident response system and conducting mock drills to better familiarize all staff in how to handle a cyber attack.
- **Get help**—Sometimes cyber-attacks are so advanced your internal IT team will not be able to thwart them. Know who you are going to call for assistance, and be sure they are available at a moment's notice; time is truly of the essence when battling cyber attackers.

Continued on Page 18 . . .

. . . Continued from Page 17

Despite your best efforts, you may be subject to a large-scale breach. Consult your insurance agent or representative to determine whether your facility has adequate cyber liability coverage. This is an important part of your preparation. ▲

_____

[1,2] Identity theft resource center breach report hits record high in 2014. Identity theft resource center Web site. http://www.idtheftcenter.org/images/breach/DataBreachReports_2014.pdf. December 31, 2014. Accessed May 8, 2015.
[3] Murphy T, Bailey B. Hackers mine for gold in medical records. *The Boston Globe*. February 6, 2015. Accessed April 28, 2015.
[4] Shahani A. The black market for stolen health care data. NPR website. http://www.npr.org/blogs/alltechconsidered/2015/02/13/385901377/the-black-market-for-stolen-health-care-data. February 13, 2015. Accessed April 28, 2015.
[5,6] Humer C, Finkle J. Your medical record is worth more to hackers than your credit card. Reuters website. http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924. September 24, 2014. Accessed April 28, 2015.
[7] Shahani A. The black market for stolen health care data. NPR website. http://www.npr.org/blogs/alltechconsidered/2015/02/13/385901377/the-black-market-for-stolen-health-care-data. February 13, 2015. Accessed April 28, 2015.
[8,9] A Winn. Cyberattacks against hospitals could kill patients or trigger terrorist attacks. International Business Times Web site. http://www.ibtimes.co.uk/cyberattacks-against-hospitals-could-kill-patients-trigger-terrorist-attacks-1508650. July 1, 2015. Accessed July 2, 2015.
[10,11,13,14] K Jackson-Higgins. Hospital medical devices used as weapons in cyberattacks. InformationWeek Dark Reading Web site. http://www.darkreading.com/vulnerabilities---threats/hospital-medical-devices-used-as-weapons-in-cyberattacks/d/d-id/1320751. June 8, 2015. Accessed July 1, 2015.
[12] Finkle J. U.S. Government probes medical devices for possible cyber flaws. Reuters Web site. http://www.reuters.com/article/2014/10/22/us-cybersecurity-medicaldevices-insight-idUSKCN0IB0DQ20141022. October 22, 2014. Accessed July 6, 2015.
[15,16,17] Eastwood B. How Boston Children's Hospital hit back at Anonymous. CIO Web site. http://www.cio.com/article/2682872/healthcare/how-boston-childrens-hospital-hit-back-at-anonymous.html. September 15, 2014. Accessed July 7, 2015.
[18] How to recognize phishing email messages, links, or phone calls. Microsoft Web site. https://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx. Accessed July 14, 2015.
[19] Radcliffe S. Patients beware: hackers are targeting your medical information. Healthline News website. http://www.healthline.com/health-news/hackers-are-targeting-your-medical-information-010715#1. January 7, 2015. Accessed April 28, 2015.
[20] http://www.dhs.gov/topic/cybersecurity, http://www.aha.org/advocacy-issues/cybersecurity.shtml, http://www.nist.gov/cyberframework/index.cfm, http://www.cms.gov.
[21] Framework for improving critical infrastructure cybersecurity. National Institute of Standards and Technology. February 12, 2014. Available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

Don't Forget AAHAM!

If you've recently had a change to your personal contact information, please let AAHAM know. If we aren't able to contact you, we can't keep you informed of all the great benefits AAHAM has to offer. So please, keep us in mind as your life changes and let us know how to reach you.

To update your AAHAM Records please contact Stephanie Hultman, Membership Chair by calling 319-240-5306, or by emailing her at sjhultman@mediacombb.net. ▲