David Ash – Chip Schutte – David Weiss - Sharon Keeler – Chuck Bishop

AGENDA
Joint Administrative Services Board
Monday August 26, 2019 1:00 p.m.
Joint Government Center

1. **Call to Order.**

2. **Approval of Minutes. (July 22 Minutes Attached).**

3. **Health Insurance Advisor.** Dr. Chuck Bishop and Tom Judge met August 6 with Ed White of McGriff Insurance Services to evaluate Clarke County's health insurance policy. We highlighted two problems with Clarke's policy: Clarke and Frederick premiums are comparable, but the employee share of family health is higher, and self only lower, than FCPS, and; CCPS PT employee share sometimes causes a negative net.

Possible Solutions:

a. Make Clarke employer share higher for family, lower for employee only.
b. Increase employer share of all coverages.
c. Separately compute retirees and make employer contribution to rate: would decrease premiums for active employees and eliminate actuarial study (average 4K annually).
d. Dependents of retiree off plan when retiree off plan.
e. Eliminate separate category for PT.
f. Push Anthem or employees on Telemedicine, wellness, chronic disease counseling to reduce premiums.
g. Increase deductible to encourage consumer behavior (eliminate KA 250). Plans are currently cross-subsidized. McGriff says most plans start at $500 deductible or more.
h. Add basic dental option; will reduce premium marginally. White skeptical of benefit.
i. Go out to bid, but problems getting data from Anthem.

4. **CyberSecurity.** At our July 22 meeting we agreed to:

a. Review VaCorp coverage *(statement of coverages attached)*;

b. Investigate vendors to educate employees *(Gordon will update us on his research)*;

c. Devise a communication to employees on end user security basics *(VaCorp has developed a webinar. This can be distributed to all employees along with other tips, but the Board should discuss how we could ensure that this communication is viewed or read).*

5. **Next Meeting September 23 (if needed).**

Joint Administrative Services Board
July 22, 2019 Regular Meeting 10:00 am

At a regular meeting of the Joint Administrative Services Board held on Monday, July 22, 2019, at 10:00 am in the Meeting Room AB, Berryville Clarke County Government Center, 101 Chalmers Court, 2nd Floor, Berryville, Virginia.

Members Present: David Ash, Sharon Keeler, David Weiss

Members Absent: Chuck Bishop, Chip Schutte

Staff Present: Tom Judge, Brian Lichty, Gordon Russell, Ed Shewbridge, Brad Shumaker, Brianna Taylor

Others Present: None

1. Call to Order - Detemination of Quorum

At 9:57 am, Vice Chairman David Weiss called the meeting to order having determined that a quorum was present.

2. Approval of Minutes

David Ash, seconded by Sharon Keeler, moved to approve the May 20, 2019 minutes as presented. The motion carried by the following voice vote:

David Ash	-	Aye
Chuck Bishop	-	Absent
Sharon Keeler	-	Aye
Chip Schutte	-	Absent
David Weiss	-	Aye

3. Health Insurance Advisor

Tom Judge stated that $2,000 was budgeted for the Health Insurance Advisor and a procurement was completed. Chuck Bishop and Tom Judge ranked the three proposals in the following order McGriff, Gallagher, and Innovative. McGriff is an insurance company located in Winchester that was formally JV Arthur; the employee representative is Ed White who was our Anthem representative in the past. The representative has experience in giving health insurance advice in this geographical area. McGriff was contacted, the price was negotiated, and ultimately they stated that they would not charge. Meeting between McGriff representative Ed White, David Ash, Chuck Bishop, and Tom Judge is set up for August 6, to have the initial conversation on how things are currently set up and what things could change to improve insurance options. Hope to have initial results for the Board by the end of August.

Vice Chair David Weiss asked what the better option was: to go with other insurance companies or to rearrange the current Local Choice methodology.

Tom Judge stated that he believed that Ed White would suggest that you would not know until you search for proposals. Tom Judge added that switching insurance is disruptive to employees and there is cost to searching other insurance companies. Unless Ed White suggests that switching insurance companies would be very beneficial then Tom Judge does not see that in the end we would risk disturbing everyone's current medical arrangements in order to leave Anthem.

4. Cybersecurity

Tom Judge Highlights:

- There have been regular episodes of security violations on systems across the country.
- End users are the ones that are attacked the most.
- Not all end users have the training to spot the attacks, which allows for easier access into the system.
- Attackers will alter an end user's computer and the end user will call IT to help. When IT is in the computer and using administrative passwords, the attacker is watching and gaining all of that information, which then can be used to hack the rest of the system.
- Need to find a way to get the employees to take the risk seriously.

Gordon Russell Highlights:

- Described the scenarios of the cases in Baltimore and Florida.
- Baltimore case all data was stolen but the locality decided not to pay the ransom, which will cost them more in the future.
- Florida case all data was stolen but the locality paid the ransom in order to try to get their data back.
- Florida case was a smaller locality (15,000 to 30,000) but the perpetrators walked away with half a million dollars.
- Expect that more small localities will be attacked.
- Combination of poor IT structure and end user email training.
- Email phishing is one of the main ways of attack; and once an end user clicks on a link, the perpetrators spend weeks in the network probing around for detailed information and steal the network data.
- Our IT strives to keep the system up to date and keep the network controlled and current, which is still not enough.
- No matter what IT does there is always the potential of risk.

- IT for both the County and the Schools feel confident in the backups and that if the system is compromised that a backup could be used to restore data.
- End users are the main target of attacks; and, if the end user is not trained, then the system network could be compromised.
- IT feels that it is important to educate all end users to the be skeptical of each and every email that comes into their inbox before they click on any links or open any attachments.
- Some ideas to improve awareness throughout the organization are reminder emails, phishing attacks, and training.
- There are companies, cost unclear, that complete these security awareness campaigns, they will attack the organization with phishing attempts and keep track of each employee over a few month period and then send a report to IT stating whether the employee passed or failed and then send helpful training tips for employees.
- There is a Google online training that is free that steps you through scenarios and tests you while you step through the process.
- This allows end users to look more in detail at the email. For example the name of who it is coming from, is the link actually the link that is written in the email, etc.
- Using same passwords at home and at work is a poor protocol to follow because then the perpetrators can get both into the work system and also attack any home devices.
- Logging out of the desktop computers at the end of each day means the computer is locked out of any user accounts and allows for any updates to be complete during the night, instead of shutting the computer down each night and having the updates occur once turned on in the morning.

Ed Shewbridge Highlights:

- School IT launched its own phishing attack about a year ago and approximately 33% of staff put in their email and password.
- Tested and trained staff to be more aware of the incoming email address and the message.
- During the phishing attack, IT discovered that one of the schools front desk personnel, who had seen the email earlier than most of the other staff, sent out an email to all staff warning them that the email that was just received did not look normal and that it should be deleted and to not click on anything within the email.
- In another school one of the teachers thought it looked different and also warned the staff.
- Found that within our buildings a few personnel are super aware of the attacks and try to warn all the other staff members.
- Constantly enforcing the safe computing practices:
    - Hardening passwords and not "remembering" them in memory.
    - Avoiding the re-use of the same password across multiple sites.
    - Logging out or sleeping computers when leaving the room.
    - Unsubscribing from SPAM emails.

    - Using encrypted websites when available.
    - Backing up data stored on individual PCs to non-networked media.
    - Restricting web surfing activity to legitimate work related sites.
- End user awareness and education is very important.
- Brad Shumaker put on a training presentation for some of the teachers to demonstrate what happens if a link is clicked on. Once they clicked on the link, Brad Shumaker showed them what he could do by having complete control over their computer.
- IT suggests that if something looks different, just delete the email. If it ends up being important, then the person will contact you in a different manner.
- Website restriction is used at the schools and there is always a struggle between restrictive and non-restrictive.
- Restrictions are different for the students and the staff. All go through the Children's Internet Protection Act (CIPA) filter but teachers have more access to websites.
- Both security awareness companies and employee educational programs are needed to better educate the end users but even then both may not be enough.
- School staff have been encouraged to use a password manager.
- Scans are being done to see what weak passwords are being used.

Next steps would be:

- Look at the cost of end user training vendors to get details, approach, and cost.
- Talk to insurance company to see mode of operation.
- Send out another reminder email to all employees with tips and tricks.

5. Next Meeting

August 26, 2019 (if needed)

6. Adjournment

At 10:49 am, Vice Chairman David Weiss adjourned the meeting.

Minutes Recorded and Transcribed by Brianna R. Taylor

TOTAL PREMIUM

	CCPS (20)	FCPS (19)	Variance
Employee	722	696.49	25.51
Family	1949	1936.6	12.4

EMPLOYER SHARE

	CCPS (20)	FCPS (19)	Variance
Employee	663.38	598.61	64.77
Family	1056.33	1263.1	-206.77

FY 20 Monthly Health Benefit Rates

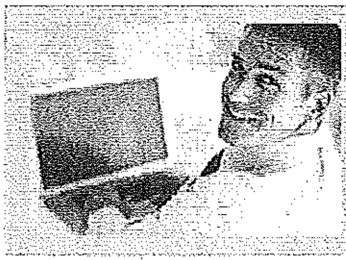
Effective 5/16/2019

Source: Joint Administrative Services

A. Plan Rates	Cost	Employer	Employee	Employer FY 20 Share*	Employer FY 19 Share*	FY 20 Employer Annual
				Rounding difference shifts year to year in KA250		
KA 250 Plan Option						
Regular Full Time						
Single	810.00	663.38	146.62	82%	84%	7,961
Dual	1,499.00	724.00	775.00	48%	50%	8,688
Family	2,187.00	1,056.33	1,130.67	48%	50%	12,676
Transportation, Food Service & Other						
Single	810.00	559.74	250.26	69%	71%	6,717
Dual	1,499.00	610.90	888.10	41%	42%	7,331
Family	2,187.00	891.31	1,295.69	41%	42%	10,696
KA 500 Plan Option						
Regular Full Time						
Single	722.00	663.38	58.62	92%	92%	7,961
Dual	1,336.00	724.00	612.00	54%	54%	8,688
Family	1,949.00	1,056.33	892.67	54%	54%	12,676
Transportation, Food Service & Other						
Single	722.00	559.74	162.26	78%	78%	6,717
Dual	1,336.00	610.90	725.10	46%	46%	7,331
Family	1,949.00	891.31	1,057.69	46%	46%	10,696
TLC High Deductible						
Regular Full Time						
Single	592.00	592.00	.00	100%	100%	7,104
Dual	1,095.00	672.99	422.01	61%	61%	8,076
Family	1,598.00	980.74	617.26	61%	61%	11,769
Transportation, Food Service & Other						
Single	592.00	499.52	92.48	84%	84%	5,994
Dual	1,095.00	567.85	527.15	52%	52%	6,814
Family	1,598.00	827.53	770.47	52%	52%	9,930
B. Account Contributions						
Regular Full Time						
TLC Health Savings Account Contribution (single)		71.38				857
TLC Health Savings Account Contribution (dual)		51.02				612
TLC Health Savings Account Contribution (family)		75.59				907
Transportation, Food Service & Other						
TLC Health Savings Account Contribution (single)		60.23				723
TLC Health Savings Account Contribution (dual)		43.05				517
TLC Health Savings Account Contribution (family)		63.78				765
C. Total Employer Cost Per Group Health Member						
Regular Full Time						
Single Health		663.38				
Dual Health		724.00				
Family Health		1,056.33				
TLC High Deductible Single Health & "HSA"		663.38				
TLC High Deductible Dual Health & "HSA"		724.00				
TLC High Deductible Family Health & "HSA"		1,056.33				
Transportation & Food Service						
Single Health		559.74				
Dual Health		610.90				
Family Health		891.31				
TLC Single Health & "HSA"		559.74				
TLC Dual Health & "HSA"		610.90			Overall Change	
TLC Family Health & "HSA"		891.31			3.40%	

Note: Where two employees are married, and they together opt for either a dual or family option, the employer will pay two times the single employer contribution for the plan option selected.

METHOD:
Force TLC High Deductible employee single contribution to zero.
Force 500 rates to percentage contributions from prior year.
Force 250 employer contribution to same as 500 contribution.
Force "HSA" contribution so total employer equal across plans.



Cyber Risk

- VACORP members are covered for online privacy matters (including identity theft), losses due to network security breaches (including hacking and viruses), copyright infringement, and online slander or libel, among other issues.

Limits

- $500,000 Per Occurrence and Aggregate - Per Member
- $5,000,000 Combined Aggregate for all Members

Coverages

Network Security, Privacy, and Data Breach Liability

- Liability for unauthorized access to the computer network, including personal identifying information such as social security numbers, credit card numbers, etc.
- Liability for transmission of a computer virus

Multimedia Liability

- Copyright/trademark infringement, invasion of privacy, plagiarism, libel and slander through website or social media

Regulatory Liability

- Liability, including defense costs, resulting from a claim by an official regulatory agency or governmental body as a result of a security breach or privacy breach or breach of privacy regulations
- Includes civil and/or administrative penalties or fines imposed by an official regulatory agency or governmental body

Data Breach Incident Response

- Expenses paid to third party service providers arising from a data breach for legal services, notification expenses, fraud monitoring and resolution services, call center services, public relations services, and computer forensic services.

Data Restoration

- Costs to restore, compile or replace data
- Reasonable and necessary costs and expenses to determine scope of breach
- Costs paid to restore, compile or replace data to a third party as a result of a network security breach or cyber extortion event

Cyber Extortion

- Reimbursement of reasonable costs and expenses resulting from request for money to avoid damage, destruction, corruption or introduction of a computer virus, a malicious code or denial of service

Social Engineering Fraud

- Covers financial loss relating to a social engineering event whereby an employee is instructed to move funds to another bank fraudulently

PCI DSS Fines Payment Card Industry Data Security Standard

- Covers PCI contractual costs and regulatory fines following a security or privacy event

Deductible

None

End User Security tips

https://member.vacorp.org/VACoRP/RiskControl/TrainingPresentation/Cyber%20Security.wmv

https://www.inc.com/neill-feather/phishing-emails-have-become-very-stealthy-here-are-5-ways-to-spot-them-every-time.html

1. Hardening passwords, and not "remembering" them in memory.
2. Logging out or sleeping computers when leaving the room.
3. Shutting down computers at night and on weekends.
4. Unsubscribing from SPAM emails.
5. Using encrypted websites when available.
6. Backing up data stored on individual PCs to non-networked media.
7. Restricting web surfing activity to legitimate work related sites.
8. Cookie and tracking management,