El Camino Health

AGENDA

COMPLIANCE AND AUDIT COMMITTEE MEETING OF THE EL CAMINO HOSPITAL BOARD

Thursday, November 19, 2020 – 5:00 pm
El Camino Hospital, 2500 Grant Road, Mountain View, CA 94040

PURSUANT TO STATE OF CALIFORNIA EXECUTIVE ORDER N-29-20 DATED MARCH 18, 2020, El CAMINO HEALTH WILL NOT BE PROVIDING A PHYSICAL LOCATION FOR THIS MEETING. INSTEAD, THE PUBLIC IS INVITED TO JOIN THE OPEN SESSION MEETING VIA TELECONFERENCE AT:
1-669-900-9128, MEETING CODE: 760-083-0558#. No participant code. Just press #.

PURPOSE: To advise and assist the El Camino Hospital (ECH) Hospital Board of Directors ("Board") in its exercise of oversight of Corporate Compliance, Privacy, Internal and External Audit, Enterprise Risk Management, and Information Technology (IT) Security. The Committee will accomplish this by monitoring the compliance policies, controls, and processes of the organization and the engagement, independence, and performance of the internal auditor and external auditor. The Committee assists the Board in oversight of any regulatory audit and in assuring the organizational integrity of ECH in a manner consistent with its mission and purpose.

	AGENDA ITEM	PRESENTED BY		ESTIMATED TIMES
1.	**CALL TO ORDER/ROLL CALL**	Sharon Anolik Shakked, Chair		**5:00 – 5:01pm**
2.	**POTENTIAL CONFLICT OF INTEREST DISCLOSURES**	Sharon Anolik Shakked, Chair		**5:01 – 5:02**
3.	**PUBLIC COMMUNICATION** a. Oral Comments *This opportunity is provided for persons in the audience to make a brief statement, not to exceed three (3) minutes on issues or concerns not covered by the agenda.* b. Written Correspondence	Sharon Anolik Shakked, Chair		**information** **5:02 – 5:05**
4.	**CONSENT CALENDAR** *Any Committee Member or member of the public may remove an item for discussion before a motion is made.* ***Approval*** a. Minutes of the Open Session of the CAC Meeting (10/01/2020) ***Information*** b. Status of FY21 Committee Goals c. Articles of Interest	Sharon Anolik Shakked, Chair	*public comment*	**motion required** **5:05 – 5:15**
5.	**REPORT ON BOARD ACTIONS** **ATTACHMENT 5**	Board Members		**information** **5:15 – 5:20**
6.	**ADJOURN TO CLOSED SESSION**	Sharon Anolik Shakked, Chair		**motion required** **5:20– 5:21**
7.	**POTENTIAL CONFLICT OF INTEREST DISCLOSURES**	Sharon Anolik Shakked, Chair		**5:21 – 5:22**
8.	**CONSENT CALENDAR** *Any Committee Member or member of the public may remove an item for discussion before a motion is made.* ***Approval*** *Gov't Code Section 54957.2:* a. Minutes of the Closed Session of the CAC Meeting (10/1/2020)	Sharon Anolik Shakked, Chair		**motion required** **5:22 – 5:40**

A copy of the agenda for the Regular Committee Meeting will be posted and distributed at least seventy-two (72) hours prior to the meeting.
In observance of the Americans with Disabilities Act, please notify us at (650) 988-7504 prior to the meeting so that we may provide the agenda in alternative formats or make disability-related modifications and accommodations.

	AGENDA ITEM	PRESENTED BY		ESTIMATED TIMES
	Information *Gov't Code Section 54956.9(d)(2)* – conference with legal counsel – pending or threatened litigation: b. KPI Scorecard and Trends c. Activity Log September 2020 d. Activity Log October 2020 e. Internal Audit Work Plan f. Internal Audit Follow Up Table g. Committee Pacing Plan			
9.	*Gov't Code Section 54956.9(d)(2)* – conference with legal counsel – pending or threatened litigation: - Enterprise Risk Management	Jim Griffith, COO; Mary Rotunno, General Counsel		**information** **5:40 – 5:50**
10.	*Gov't Code Section 54956.9(d)(2)* – conference with legal counsel – pending or threatened litigation: - IT Security Discussion	Deb Muro, CIO; Mary Rotunno, General Counsel		**discussion** **5:50 – 6:20**
11.	*Gov't Code Section 54956.9(d)(2)* – conference with legal counsel – pending or threatened litigation: - Email Retention Procedures	Diane Wigglesworth, Sr. Director Corporate Compliance; Mary Rotunno, General Counsel		**discussion** **6:20 – 6:35**
12.	*Gov't Code Section 54956.9(d)(2)* – conference with legal counsel – pending or threatened litigation: Report on Internal Audit Activity	Diane Wigglesworth, Sr. Director, Corporate Compliance; Mary Rotunno, General Counsel		**information** **6:35 – 6:40**
13.	*Gov't Code Sections 54957* for report and discussion on personnel matters – Senior Management: - Executive Session	Sharon Anolik Shakked, Chair		**discussion** **6:40 – 6:50**
14.	**ADJOURN TO OPEN SESSION**	Sharon Anolik Shakked, Chair		**motion required** **6:50 – 6:51**
15.	**RECONVENE OPEN SESSION/ REPORT OUT** To report any required disclosures regarding permissible actions taken during Closed Session.	Sharon Anolik Shakked, Chair		**information** **6:51 – 6:55**
16.	**ADJOURNMENT**	Sharon Anolik Shakked, Chair		**motion required** **6:55 – 7:00pm**

Upcoming Meetings:

Regular Meetings:

January 28, 2021

March 18, 2021

April 28, 2021 (Joint Board and Committee Educational Session)

May 20, 2021

Minutes of the Open Session of the
Compliance and Audit Committee
of the El Camino Hospital Board of Directors
Thursday, October 1, 2020
El Camino Hospital | 2500 Hospital Drive, Mountain View, CA 94040

Members Present**	**Members Absent**
Sharon Anolik Shakked, Chair	
Lica Hartman	
Jack Po, MD, Vice Chair	
Christine Sublett	
Julia Miller	

****All via teleconference**

Agenda Item	Comments/Discussion	Approvals/ Action
1. CALL TO ORDER/ ROLL CALL	The open session meeting of the Compliance and Audit Committee of El Camino Hospital ("the Committee") was called to order at 5:00pm by Chair Anolik Shakked. All Committee members participated via teleconference and were present at roll call. A quorum was present pursuant to State of California Executive Orders N-25-20 dated March 12, 2020 and N-29-20 dated March 18, 2020.	***Called to order at 5:00pm***
2. POTENTIAL CONFLICT OF INTEREST	Chair Anolik Shakked asked if any Committee members had a conflict of interest with any of the items on the agenda. No conflicts were reported.	
3. PUBLIC COMMUNICATION	None.	
4. CONSENT CALENDAR	Chair Anolik Shakked asked if any member of the Committee or the public wished to remove any agenda items from the consent calendar. No requests were reported. **Motion:** To approve the consent calendar a) Minutes of the Open Session of the Compliance and Audit Committee Meeting (08/20/2020); and for information: b) Status of FY21 Committee Goals **Movant:** Miller **Second:** Sublett **Ayes:** Anolik Shakked, Hartman, Miller, Po, & Sublett **Noes:** None **Abstentions:** None **Absent:** None **Recused:** None	***Consent Calendar approved***
5. REPORT ON BOARD ACTIONS	Jack Po, M.D. reported on the board actions and discussed materials as presented in the packet. Chair Anolik Shakked asked if any Committee members had any questions about the Report on Board Actions. No questions were reported.	
6. COMMITTEE SELF-ASSESSMENT RESULTS	Cindy Murphy, Director, Governance Services, reported on the results of the Committee Self-Assessment as presented in the packet. In response to committee members' questions, Ms. Murphy reported that another Committee had moved the Report on Board Actions to the consent calendar and replaced it with a Chair's report to enable the Committee to (1) receive more information about the work of the Board and (2) save time for discussion about important issues. In regards to turnover issues within the CAC committee, Ms. Miller volunteered to talk to the Board Chair, and Ms. Murphy offered to remind	

	the Board Chair about the frequent turnover of Board members serving on the Committee when FY22's slate is developed in June. Dr. Po suggested bringing more community members into the Compliance and Audit Committee. Chair Anolik Shakked asked if any members had any comments or suggestions about either having more meetings, making the meetings longer, or looking into putting some lesser important topics for the consent calendar to enable more time for discussion of important issues facing the Committee. Ms. Hartman suggested looking into discussing the more important topics within the current scheduled meetings and not making meetings longer than normal. Chair Anolik Shakked reported that she and Ms. Wigglesworth had discussed placing the KPI, Scorecard, and Trends Report, Internal Audits with no findings or very low findings, and the Internal Audit Follow-Up on the consent calendar. Other members agreed with these suggestions. Chair Anolik Shakked suggested including Article(s) of Interest to the Consent Calendar for information to satisfy the Committee's interest in education on specific topics mentioned in the Self- Assessment Report.	
7. KPIs, SCORECARD, AND TRENDS	Chair Anolik Shakked asked if any members of the committee had any questions regarding the information provided in the packet. In response to a committee member's questions, Ms. Wigglesworth stated that management requires that all new employees' healthstream training be completed within 30 days of their date of hire. In the packet, 100% means that the organization has been 100% compliant with that requirement. Chair Anolik Shakked suggested Ms. Wigglesworth provide new Committee members with a one page document during onboarding that explains and will orient them on how to read the scorecard.	
8. ADJOURN TO CLOSED SESSION	**Motion:** To adjourn to closed session at 5:50pm. **Movant:** Miller **Second:** Po **Ayes:** Anolik Shakked, Hartman, Miller, Po, & Sublett **Noes:** None **Abstentions:** None **Absent:** None **Recused:** None	***Adjourned to closed session at 5:50pm***
9. AGENDA ITEM 17: RECONVENE OPEN SESSION/ REPORT OUT	Open session was reconvened at 7:20pm. Agenda items 9-16 were discussed in closed session. During the closed session, the Committee approved the Minutes of the Closed Session of the Compliance and Audit Committee Meeting (08/20/20) with a minor amendment and the Financial Audit Results.	***Open session reconvened at 7:20pm***
10. AGENDA ITEM 18: ADJOURNMENT	**Motion:** To adjourn at 7:22pm. **Movant:** Po **Second:** Sublett **Ayes:** Anolik Shakked, Hartman, Miller, Po, & Sublett **Noes:** None **Abstentions:** None **Absent:** None **Recused:** None	***Meeting adjourned at 7:22pm***

Attest as to the approval of the foregoing minutes by the Compliance and Audit Committee of El Camino Hospital:

_____
Sharon Anolik Shakked
Chair, Compliance and Audit Committee

El Camino Health

FY21 COMMITTEE GOALS

Compliance and Audit Committee

PURPOSE

The purpose of the Compliance and Audit Committee (the "Committee") is to advise and assist the El Camino Hospital (ECH) Hospital Board of Directors ("Board") in its exercise of oversight of Corporate Compliance, Privacy, Internal and External Audit, Enterprise Risk Management, and Information Technology (IT) Security. The Committee will accomplish this by monitoring the compliance policies, controls, and processes of the organization and the engagement, independence, and performance of the internal auditor and external auditor. The Committee assists the Board in oversight of any regulatory audit and in assuring the organizational integrity of ECH in a manner consistent with its mission and purpose.

STAFF: **Diane Wigglesworth**, Sr. Director, Corporate Compliance (Executive Sponsor)

The Sr. Director, Corporate Compliance shall serve as the primary staff to support the Committee and is responsible for drafting the Committee meeting agenda for the Committee Chair's consideration. Additional members of the Executive Team or outside consultants may participate in the meetings upon the recommendation of the Executive Sponsor and at the discretion of the Committee Chair.

GOALS	TIMELINE	METRICS
1. Review Hospital and SVMD Compliance Work Plan for FY 2021.	Q1 FY21	Committee reviews and provides recommendations to the Compliance Officer.
2. Review Business Continuity and Disaster Recovery Plan with focus on effectiveness and appropriateness of COVID – 19 pandemic response and recovery.	Q3 FY21	Committee reviews and provides a report to the Board and recommendations to the COO that include assessment of COVID-19 response and recovery as well as a look back at preparedness had the anticipated "surge" occurred in FY 20 Q3 and Q4.
3. Participate in education session presented by Legal Counsel regarding revisions to Stark Law and Anti-Kickback Statute	~~Q3 FY21~~ - TBD	Committee receives education and recommends information to be presented to the Board. (Issuing of final rules delayed until August 2021)
4. Review ECH's IT Security Strategic Plan.	Q4 FY21	Committee reviews and provides recommendations to CIO.

SUBMITTED BY:

Chair: Sharon Anolik Shakked
Executive Sponsor: Diane Wigglesworth

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments[1]

Date: October 1, 2020

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is issuing this advisory to highlight the sanctions risks associated with ransomware payments related to malicious cyber-enabled activities. Demand for ransomware payments has increased during the COVID-19 pandemic as cyber actors target online systems that U.S. persons rely on to continue conducting business. Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC regulations. This advisory describes these sanctions risks and provides information for contacting relevant U.S. government agencies, including OFAC, if there is a reason to believe the cyber actor demanding ransomware payment may be sanctioned or otherwise have a sanctions nexus.[2]

Background on Ransomware Attacks

Ransomware is a form of malicious software ("malware") designed to block access to a computer system or data, often by encrypting data or programs on information technology systems to extort ransom payments from victims in exchange for decrypting the information and restoring victims' access to their systems or data. In some cases, in addition to the attack, cyber actors threaten to publicly disclose victims' sensitive files. The cyber actors then demand a ransomware payment, usually through digital currency, in exchange for a key to decrypt the files and restore victims' access to systems or data.

In recent years, ransomware attacks have become more focused, sophisticated, costly, and numerous. According to the Federal Bureau of Investigation's 2018 and 2019 Internet Crime Reports, there was a 37 percent annual increase in reported ransomware cases and a 147 percent annual increase in associated losses from 2018 to 2019.[3] While ransomware attacks are carried out against large corporations, many ransomware attacks also target small- and medium-sized

[1] This advisory is explanatory only and does not have the force of law. It does not modify statutory authorities, Executive Orders, or regulations. It is not intended to be, nor should it be interpreted as, comprehensive or as imposing requirements under U.S. law, or otherwise addressing any particular requirements under applicable law. Please see the legally binding provisions cited for relevant legal authorities.

[2] This advisory is limited to sanctions risks related to ransomware and is not intended to address issues related to information security practitioners' cyber threat intelligence-gathering efforts more broadly. For guidance related to those activities, see guidance from the U.S. Department of Justice, Criminal Division, Computer Crime and Intellectual Property Section, Cybersecurity Unit, *Legal Considerations when Gathering Online Cyber Threat Intelligence and Purchasing Data from Illicit Sources* (February 2020), available at https://www.justice.gov/criminal-ccips/page/file/1252341/download.

[3] *Compare* Federal Bureau of Investigation, Internet Crime Complaint Center, *2018 Internet Crime Report*, at 19, 20, available at https://pdf.ic3.gov/2018_IC3Report.pdf, *with* Federal Bureau of Investigation, Internet Crime Complaint Center, *2019 Internet Crime Report*, available at https://pdf.ic3.gov/2019_IC3Report.pdf.

businesses, local government agencies, hospitals, and school districts, which may be more vulnerable as they may have fewer resources to invest in cyber protection.

OFAC Designations of Malicious Cyber Actors

OFAC has designated numerous malicious cyber actors under its cyber-related sanctions program and other sanctions programs, including perpetrators of ransomware attacks and those who facilitate ransomware transactions. For example, starting in 2013, a ransomware variant known as Cryptolocker was used to infect more than 234,000 computers, approximately half of which were in the United States.[4] OFAC designated the developer of Cryptolocker, Evgeniy Mikhailovich Bogachev, in December 2016.[5]

Starting in late 2015 and lasting approximately 34 months, SamSam ransomware was used to target mostly U.S. government institutions and companies, including the City of Atlanta, the Colorado Department of Transportation, and a large healthcare company. In November 2018, OFAC designated two Iranians for providing material support to a malicious cyber activity and identified two digital currency addresses used to funnel SamSam ransomware proceeds.[6]

In May 2017, a ransomware known as WannaCry 2.0 infected approximately 300,000 computers in at least 150 countries. This attack was linked to the Lazarus Group, a cybercriminal organization sponsored by North Korea. OFAC designated the Lazarus Group and two sub-groups, Bluenoroff and Andariel, in September 2019.[7]

Beginning in 2015, Evil Corp, a Russia-based cybercriminal organization, used the Dridex malware to infect computers and harvest login credentials from hundreds of banks and financial institutions in over 40 countries, causing more than $100 million in theft. In December 2019, OFAC designated Evil Corp and its leader, Maksim Yakubets, for their development and distribution of the Dridex malware.[8]

OFAC has imposed, and will continue to impose, sanctions on these actors and others who materially assist, sponsor, or provide financial, material, or technological support for these activities.

---

[4] Press Release, U.S. Dept. of Justice, U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator (June 2, 2014), available at https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware.

[5] Press Release, U.S. Dept. of the Treasury, Treasury Sanctions Two Individuals for Malicious Cyber-Enabled Activities (Dec. 29, 2016), available at https://www.treasury.gov/press-center/press-releases/Pages/jl0693.aspx.

[6] Press Release, U.S. Dept. of the Treasury, Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses (Nov. 28, 2018), available at https://home.treasury.gov/news/press-releases/sm556.

[7] Press Release, U.S. Dept. of the Treasury, Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups (Sept. 13, 2019), available at https://home.treasury.gov/news/press-releases/sm774.

[8] Press Release, U.S. Dept. of the Treasury, Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware (Dec. 5, 2019), available at https://home.treasury.gov/news/press-releases/sm845.

Ransomware Payments with a Sanctions Nexus Threaten U.S. National Security Interests

Facilitating a ransomware payment that is demanded as a result of malicious cyber activities may enable criminals and adversaries with a sanctions nexus to profit and advance their illicit aims. For example, ransomware payments made to sanctioned persons or to comprehensively sanctioned jurisdictions could be used to fund activities adverse to the national security and foreign policy objectives of the United States. Ransomware payments may also embolden cyber actors to engage in future attacks. In addition, paying a ransom to cyber actors does not guarantee that the victim will regain access to its stolen data.

Facilitating Ransomware Payments on Behalf of a Victim May Violate OFAC Regulations

Under the authority of the International Emergency Economic Powers Act (IEEPA) or the Trading with the Enemy Act (TWEA),[9] U.S. persons are generally prohibited from engaging in transactions, directly or indirectly, with individuals or entities ("persons") on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List), other blocked persons, and those covered by comprehensive country or region embargoes (e.g., Cuba, the Crimea region of Ukraine, Iran, North Korea, and Syria). Additionally, any transaction that causes a violation under IEEPA, including transactions by a non-U.S. person which causes a U.S. person to violate any IEEPA-based sanctions, is also prohibited. U.S. persons, wherever located, are also generally prohibited from facilitating actions of non-U.S. persons, which could not be directly performed by U.S. persons due to U.S. sanctions regulations. OFAC may impose civil penalties for sanctions violations based on strict liability, meaning that a person subject to U.S. jurisdiction may be held civilly liable even if it did not know or have reason to know it was engaging in a transaction with a person that is prohibited under sanctions laws and regulations administered by OFAC.

OFAC's Economic Sanctions Enforcement Guidelines (Enforcement Guidelines)[10] provide more information regarding OFAC's enforcement of U.S. economic sanctions, including the factors that OFAC generally considers when determining an appropriate response to an apparent violation. Under the Enforcement Guidelines, in the event of an apparent violation of U.S. sanctions laws or regulations, the existence, nature, and adequacy of a sanctions compliance program is a factor that OFAC may consider when determining an appropriate enforcement response (including the amount of civil monetary penalty, if any).

As a general matter, OFAC encourages financial institutions and other companies to implement a risk-based compliance program to mitigate exposure to sanctions-related violations.[11] This also applies to companies that engage with victims of ransomware attacks, such as those involved in providing cyber insurance, digital forensics and incident response, and financial services that may involve processing ransom payments (including depository institutions and money services

[9] 50 U.S.C. §§ 4301–41; 50 U.S.C. §§ 1701–06.
[10] 31 C.F.R. part 501, appx. A.
[11] To assist the public in developing an effective sanctions compliance program, in 2019, OFAC published *A Framework for OFAC Compliance Commitments*, intended to provide organizations with a framework for the five essential components of a risk-based sanctions compliance program. The *Framework* is available at https://home.treasury.gov/system/files/126/framework_ofac_cc.pdf.

businesses). In particular, the sanctions compliance programs of these companies should account for the risk that a ransomware payment may involve an SDN or blocked person, or a comprehensively embargoed jurisdiction. Companies involved in facilitating ransomware payments on behalf of victims should also consider whether they have regulatory obligations under Financial Crimes Enforcement Network (FinCEN) regulations.[12]

Under OFAC's Enforcement Guidelines, OFAC will also consider a company's self-initiated, timely, and complete report of a ransomware attack to law enforcement to be a significant mitigating factor in determining an appropriate enforcement outcome if the situation is later determined to have a sanctions nexus. OFAC will also consider a company's full and timely cooperation with law enforcement both during and after a ransomware attack to be a significant mitigating factor when evaluating a possible enforcement outcome.

OFAC Licensing Policy

Ransomware payments benefit illicit actors and can undermine the national security and foreign policy objectives of the United States. For this reason, license applications involving ransomware payments demanded as a result of malicious cyber-enabled activities will be reviewed by OFAC on a case-by-case basis with a presumption of denial.

Victims of Ransomware Attacks Should Contact Relevant Government Agencies

OFAC encourages victims and those involved with addressing ransomware attacks to contact OFAC immediately if they believe a request for a ransomware payment may involve a sanctions nexus. Victims should also contact the U.S. Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection if an attack involves a U.S. financial institution or may cause significant disruption to a firm's ability to perform critical financial services.

- U.S. Department of the Treasury's Office of Foreign Assets Control
  - Sanctions Compliance and Evaluation Division: ofac_feedback@treasury.gov; (202) 622-2490 / (800) 540-6322
  - Licensing Division: https://licensing.ofac.treas.gov/; (202) 622-2480
- U.S. Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP)
  - OCCIP-Coord@treasury.gov; (202) 622-3000
- Financial Crimes Enforcement Network (FinCEN)
  - FinCEN Regulatory Support Section: frc@fincen.gov

[12] *See* FinCEN Guidance, FIN-2020-A00X, "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments," October 1, 2020, for applicable anti-money laundering obligations related to financial institutions in the ransomware context.

Contact Information for Other Relevant U.S. Government Agencies:

- Federal Bureau of Investigation Cyber Task Force
  - https://www.ic3.gov/default.aspx; www.fbi.gov/contact-us/field
- U.S. Secret Service Cyber Fraud Task Force
  - www.secretservice.gov/investigation/#field
- Cybersecurity and Infrastructure Security Agency
  - https://us-cert.cisa.gov/forms/report
- Homeland Security Investigations Field Office
  - https://www.ice.gov/contact/hsi

If you have any questions regarding the scope of any sanctions requirements described in this advisory, please contact OFAC's Sanctions Compliance and Evaluation Division at (800) 540-6322 or (202) 622-2490.

How hackers negotiated with UCSF for $1M+ ransom: 5 things to know

Jackie Drees - Wednesday, July 1st, 2020 Print | Email

Ransomware gang Netwalker attacked the University of California San Francisco medical school's computer systems June 1, initially demanding a $3 million ransom, according to *BBC News*.

After negotiations with Netwalker, UCSF paid $1.14 million in ransom to unlock the servers and data the hackers encrypted. Due to an anonymous tip, *BBC News* was able to follow the negotiations between UCSF and Netwalker in a live chat on the dark web.

When it comes to paying ransoms, cybersecurity expert Jan Op Gen Oorth from Europol said victims should not pay because it encourages criminals to continue inflicting ransomware on others, while Brett Callow, a threat analyst at cybersecurity company Emsisoft said that "organizations in this situation are without a good option."

Five things to know about Netwalker's dark website and how it negotiates with victims:

1. The website resembles a "standard customer-service website" and features a frequently asked questions tab, a live chat option and a "free" sample of its software.

2. The website includes a countdown timer that ticks down to a time when Netwalker either deletes the data they infected with malware or doubles the price of the ransom.

3. UCSF was instructed to log in to Netwalker's website for negotiations either by email or a ransom note left on the hacked computer screens. After a day of negotiations on June 5, UCSF made a final offer of $1.14 million and the next day transferred the amount in bitcoin to Netwalker's electronic wallets.

4. UCSF told *BBC News* that it paid the ransom because "the data that was encrypted is important to some of the academic work we pursue as a university serving the public good," adding, "It would be a mistake to assume that all of the statements and claims made in the negotiations are factually accurate."

5. Most ransomware attacks start through email phishing, and research suggests that cyber criminals are using tools that gain access to systems via a single download.

Click here to view the full report.

More articles on cybersecurity:
Clinic employee takes phishing bait, may have exposed 19,000 patients' info: 4 details
UnityPoint Health to pay $2.8M+ settlement over phishing attacks: 6 details
10 health system malware, ransomware and phishing incidents this month

El Camino Health

EL CAMINO HOSPITAL BOARD OF DIRECTORS
COMMITTEE MEETING MEMO

To: Compliance and Audit Committee
From: Cindy Murphy, Director of Governance Services
Date: November 19, 2020
Subject: Report on Board Actions

Purpose: To keep the Committee informed with regards to actions taken by the El Camino Hospital and El Camino Healthcare District Boards.

Summary:

1. Situation: It is important to keep the Committees informed about Board activity to provide context for Committee work. The list below is not meant to be exhaustive, but includes agenda items the Board voted on that are most likely to be of interest to or pertinent to the work of El Camino Hospital's Board Advisory Committees.

2. Authority: This is being brought to the Committees at the request of the Board and the Committees.

3. Background: Since the last time we provided this report to the Compliance and Audit Committee, the Hospital Board has met twice and the District Board has met twice. In addition, since the Board has delegated certain authority to the Executive Compensation Committee, the Compliance and Audit Committee and the Finance Committee, those approvals are also noted in this report.

Board/Committee	**Meeting Date**	**Actions** (Approvals unless otherwise noted)
ECH Board	October 14, 2020	- Resolution Recognizing the El Camino Health Foundation for Establishing COVID-19 Relief Fund - FY21 Period 2 Financials - FY20 Financial Audit and Cash Balance and 403(b) Plan Audits - Quality Committee Report Including Credentials and Privileges Report - FY20 Organizational Performance Score - FY21 Readmissions Organizational Performance Goal Metrics - Neuro-Interventional Call Panel - Medical Director, Cardiac Rehabilitation
	November 11, 2020	- Resolution 2020-10 Recognizing Brian Richards' Service to the Organization - Medical Staff Report - Quality Council Minutes - Medical Staff Credentials and Privileges Report - Election of Carlo Bohorquez, CFO and Deb Muro, CIO to the Pathways Home Health and Hospice Board of Directors - Pathways FY21 Budget - FY21 Board Action Plan - Revised Policy and Procedures for Nomination and Appointment of Community Members to the Board's

Board/Committee	**Meeting Date**	**Actions** (Approvals unless otherwise noted)
		Advisory Committees - FY21 Board Retreat Agenda - Annual Safety Report for the Environment of Care - FY21 CEO Base Salary - FY20 CEO Incentive Compensation Payout
ECHD Board	October 20, 2020	- FY20 Year End Consolidated Financials - FY20 Year End Community Benefit Report - ECHD Conflict of Interest Code - FY20 Year End ECHD Stand Alone Financials - FY20 Financial Audit - FY21 Period 2 Financials - Appointment of District Director George Ting as Chair of the ECH Board Member Election Ad Hoc Committee and as Liaison to the Community Benefit Advisory Council - Revisions to the ECHD Community Benefit Grants Policy (moves up timeline for notification to the public regarding grant funding cycle)
Executive Compensation Committee	September 22, 2020	- FY21 Executive Base Salaries - FY21 Executive Individual Goals FY21 Executive Compensation Incentive Payouts
	November 5, 2020	- FY21 CFO Individual Performance Goals - Renewal of Executive Compensation Consultant Contract
Compliance and Audit Committee	N/A	
Finance Committee	N/A	

List of Attachments: None.

Suggested Committee Discussion Questions: None.