City and County of San Francisco
Edwin M. Lee, Mayor
San Francisco Department of Public Health
Barbara A. Garcia, Director of Health

DPH Business Ethics and Best Practices
All Staff Memo
September 23, 2016

To protect critical data, use of personal email software programs will be blocked on the SFDPH Network beginning October 23, 2016

There have been several media reports of hacking and ransomware involving health care organizations. Healthcare organizations are increasingly targeted by cybercriminals because of the importance of healthcare information.

Ransomware is a type of malware that infects computer systems, restricting users' access to the infected systems. Criminals often attempt to extort money from victims by displaying an on-screen alert. Typically, these alerts state that the user's systems have been locked or that the user's files have been encrypted. Users are told that unless a ransom is paid, access will not be restored. A California hospital was attacked with ransomware in February 2016 and was forced to divert critical 911 patients to other medical centers and to administer care without access to the important information contained in electronic medical records. This disruption occurred for over a week. The hospital ended up paying a ransom of thousands of dollars to regain access to their systems.

Ransomware and viruses are often spread through phishing emails that contain malicious attachments. As a reminder, **please do not open any suspicious emails or attachments in your DPH email.** Instead, report it to the DPH Help Desk (415-759-3577). These harmful attachments can access your computer files and the DPH network. Hackers also access healthcare information systems when users access malicious websites.

To discourage these types of cyberattacks, the San Francisco Department of Public Health (SFDPH) has had a longstanding policy prohibiting use of the DPH-issued devices for personal use including accessing personal email accounts. **Effective October 23, 2016, SFDPH will prohibit and block user access to Third Party Email (TPE) applications such as Gmail, Yahoo, etc. while operating on the SFDPH network; e.g., on your office computer and/or via remote access.**

If you have a business need to access a TPE, please contact the Office of Compliance and Privacy Affairs at (1-855-792-6040) to request an exception.

Thank you for protecting the personal information of the individuals we serve and for maintaining the safety and security of our data systems. **See Frequently Asked Questions (FAQs) on next page.**

To protect critical data, use of personal email software programs will be blocked on the SFDPH Network beginning October 23, 2016

Use of Third Party Email (TPE) Applications
Frequently Asked Questions

#	Question	Answer
1	What is a Third Party Email (TPE)?	Gmail, Yahoo, Hotmail, AOL or other personal email system applications
2	What is a device?	A personal or SFDPH-issued cell phone, tablet, laptop, computer, etc.
3	What is the SFDPH network?	The place where you are taken once you log on to your computer at work or remotely through a token (VPN).
4	May I access my TPE via the internet while I am signed on to the SFDPH network on my office computer? At home via a token?	Either way, no. It is against SFDPH policy and, effective October 23, 2016, you will be blocked from doing so.
5	I use a SFDPH computer and access my TPE on the SFDPH network because I do not have a SFDPH email account. I need to send messages for work purposes. Now what?	Notify your supervisor that you need a SFDPH-issued email account. All individuals needing to conduct SFDPH business on a SFDPH-issued device via email should be issued a SFDPH email account.
6	I have a SFDPH-issued email account but I need to use a TPE for SFDPH business because (give reason). What should I do?	Notify the Office of Compliance and Privacy Affairs at compliance.privacy@sfdph.org or 855-729-6040 to request an exception to this policy.
7	I use my own personal device (cell phone, tablet or laptop) to access my SFDPH Outlook email account. Is there any danger if I also access TPEs on my personal device?	No, there is no danger to SFDPH data security when you use your personal device to access your TPE. (Note: If a DPH email contains PHI, all privacy policies and regulations apply in the handling of that emailed PHI even if the email is opened on a personal device.)
8	I have a DPH-issued device (cell phone, tablet or laptop). May I access TPEs on it if I am not on the network?	No, although not a security risk, SFDPH-issued devices may not be used for personal use.
9	I need to send an email from my personal device to my work computer. Is that allowable?	Yes, it is fine for SFDPH Outlook to receive emails from TPEs as there is enhanced encryption capabilities in SFDPH Outlook.
10	Staff in my program use Google calendar and share it with others inside and outside SFDPH. Is that allowable?	Yes, for the time being only email access will be blocked. Use of google calendar will be allowed until we transition to Outlook's Calendar.
11	Staff in my program use Doodle, Google Doc, Google Analytics and Google Drive. Is that allowable?	Yes, these programs will not be blocked….only access to third party email systems will be blocked.

If you have further questions, please feel free to contact the DPH IT Help Desk at 415-759-3577.