COLORADO
Department of Health Care Policy & Financing

Colorado Department of Health Care Policy & Financing Standard Operating Procedure

Number: ADM-013

ELECTRONIC MAIL (EMAIL) POLICY

I. Purpose and Authority

A. Purpose: The purpose of this Standard Operating Procedure (SOP) is to establish policy and procedure for all workforce members and to set forth guidelines and standards on the proper use of the electronic mail system provided by the department. This SOP aims to make users aware of their rights and responsibilities regarding the use of electronic mail communication systems and ensure the use of electronic mail and associated equipment is consistent with applicable law and Department policies.

B. Authority:

45 C.F.R. § 160.103; 45 C.F.R. §164.501; 45 C.F.R. § 164.514(b)(2); AND SOP PSP-032, Encryption of Workstation, Laptops, Email, and Mobile Computing Devices.

C.R.S. § 24-37.5-101 through 106, which establishes the Governor's Office of Information Technology to provide state agencies with enterprise technology services.

C.R.S. § 24-72-201, *et seq.*, the Colorado Open Records Act (CORA); and SOP ADM-029 Public (Open) Records Requests Pursuant to the Colorado Open Records Act (CORA)

C.R.S. § 24-73-101, *et seq.*, the Colorado Data Protection law that requires agencies to establish a policy for the retention, maintenance, and destruction of electronic records which contain personal identifying information (PII).

Colorado Department of Personnel, State Archives, *State Agencies Records Management Manual*.

II. Definitions

For this SOP, the terms in this section are construed and interpreted as follows:

A. Electronic Mail (Email): an electronic message that is transmitted between two or more computers or electronic terminals, regardless of whether the message is converted to hard copy format after whether the message is viewed upon transmission or stored for later retrieval. "Electronic mail" includes electronic messages that are transmitted through a local, regional, or global computer network, as defined by C.R.S. § 24-72-202(1.2).

B. Governor's Office of Information Technology (OIT): The state agency responsible for the operations and delivery of information and communications technology (ICT) services and innovation across all executive branch agencies in the State of Colorado.

C. Google Email (Gmail): A web-based application that enables a user to manage their e-mail mailbox, calendar, contacts, and other Google features online.

D. HIPPA: For purposes of this SOP, HIPAA is defined as the health insurance portability and accountability act of 1996, 45 U.S.C. §§ 1320d-1320d-8, and its implementing regulations promulgating by the U.S. Department of Health and Human Services, 45 C.F.R. Parts 160 and 164, and other applicable laws, as amended.

E. Personal Identifying Information (PII): Means a Social Security number; A personal identification number; A password; A passcode; an official state or government issued driver's license or identification card number; a government passport number; Biometric data, as defined in section 24-73-103 (1)(a); an employer, student, or military identification number; for a financial transaction device, as defined in section 18-5-701(3).

F. Protected Health Information (PHI): Individually identifiable health information that is (1) transmitted by electronic media; (2) maintained in electronic media; or (3) transmitted or maintained in any other form or medium. *See* 45 C.F.R.

G. Workforce: Permanent and temporary employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the Department, is under the direct control of the Department, whether or not they are paid by the Department.

III. Policy

A. Department computer systems, including electronic mail (email)platforms or capabilities, are for official state business. Workforce members are not authorized

to use the Department's e-mail communications platforms or capabilities for personal profit or gain.

B. All e-mail communications and associated attachments transmitted form, received by, or stored on any equipment owned by the state or the property of the Department and, as such, are subject to the provisions of this policy.

C. The Department reserves the right to monitor the e-mail communications of its workforce members to ensure that the computer systems are not being used for unlawful purposes or in a manner otherwise prohibited by this policy. Such monitoring, with written authorization from the workforce members division director, may include tracking addresses of mail sent and received, assessing inbox messages, assessing messages in folders, and assessing archived messages. Users should not expect the Department to obtain their consent before assessing or disclosing the content of e-mail communications.

D. The Department may take the appropriate corrective action, including discipline and/or termination of workforce members, based on information obtained from monitoring or inspecting electronic mail communications.

E. Pursuant to C.R.S § 24-72-203, Electronic mail that is written in the conduct of public business is deemed a public record and, unless specifically exempted under the Colorado Open Records Act, is subject to disclosure. This could be true, regardless of whether the communication was sent or received on a public or privately owned personal computer. Therefore, any electronic mail that is written in the conduct of public business by a workforce member is subject to the provisions of this policy. *See* SOP PSP-032, Encryption of Workstation, Laptops, Email, and Mobile Computing Devices.

F. The Department may disclose email communications sent to, received by, or relating to law enforcement officials or others without giving prior notice to the workforce member.

IV. Procedure

A. Emails About Private or Confidential Matters: Circulation of attorney-client privileged, or attorney work product communications should be limited to Department personnel with a “need to know” and remain WITHIN THE AGENCY. Some e-mail communications, especially those with the Colorado Attorney General's Office or concerning litigation or other legally sensitive matters, may be entitled to the confidential treatment and be exempt from the public disclosure under the Colorado Open Records Act. Sharing an attorney client privileged

document outside the agency, even with a "selected audience "may waive the privilege and render the document a public record subject to disclosure to any member of the public. Therefore, Department personnel communicating with the Colorado Attorney General's Office may place the claim of privilege at the top of such communications as followed:

1. Privileged-Attorney-Client Communication. Do not place in central or unrestricted files. Any circulation or distribution to persons outside the agency may waive the privilege.

B. Forwarding Messages: Users should be aware that they have no control over what the recipient of a message does with that message once it is in the recipient's possession. When writing an electronic mail communication, keep in mind that the intentional or accidental forwarding of a communication is always a possibility. If you choose to forward an e-mail message to a third party that was originally addressed to you, either forward the message unchanged or distinctly identify any modifications you have made. It is also recommended that you always retain forwarding information, so that the original author of the forwarded message can be easily identified. If you are preparing an e-mail that you do not want to be forwarded or the distribution of which should be restricted, clearly mark the message, as appropriate,

1. "Do Not Forward" or

2. "Not for Distribution Outside the Agency"

If you wish to forward a message, it is always a good practice to ask for the author's permission.

C. Public Release of Information: The release of any emails or electronic information to the public, as set forth in the Colorado Open Records Act (CORA), shall not occur without the Department's CORA Officer. Formal requests for release of public records under CORA will be handled by the Department's CORA Officer, and may be discussed with your manager and the Legal Division. Workforce member should identify emails which contain PHI/PII or attorney-client privileged information to the CORA Officer. The Open Records Act has specific response time requirements and sanctions for noncompliance. See SOP ADM-029, Public (open) Records Requests Pursuant to the Colorado Open Records Act (CORA).

1. Email messages marked "Privileged Attorney-Client Communications," or that deal with matters in litigation or are otherwise legally sensitive, should not be

released without prior consultation with the Department's attorneys at the Colorado Attorney General's Office or the Legal Division Director.

2. Email marked "DO Not Forward" should not be forwarded without approval from the sender or other person who placed the restriction on the message (or their supervisor).

3. Email marked "Not for Distribution Outside the Agency" should not be forwarded outside the agency forwarded without approval from the sender or other person who placed the restriction on the message (or their supervisor).

D. Filing and Retention: The manner in which e-mail messages are initially handled when they arrive in a workforce members mailbox is left to their discretion, except where regulations require retention or other special handily. Please see direction provided in policies on Acceptable Use and Retention (SOP PSP-018 Workstation Acceptable Use) and (SOP ADM-014 Records Maintenance, Storage and Retention (Archiving)). The workforce member can do the following:

1. Read and delete the message,

2. read and then save or print the message and/or attachments outside the mailbox, or

3. read and then save the message in the mailbox.

All electronic mail messages in the users Google mailbox (Gmail) older than 90 days will be automatically deleted, and messages in the Gmail trash folder older than 30 days will automatically be permanently deleted. it is the responsibility of the workforce member to take necessary actions (e.g., applying the DONOTDELETE label two the e-mail, saving messages to another file server location, or printing the message to hardcopy) to save e-mail messages if such information must be retained beyond the Department's e-mail retention period.

Emails that are labeled DONOTDELETE within the workforce members Google mail (Gmail) account or saved locally on their hard drive or another file storage location, will not be subject to the above age limitations that are applied on the Gmail account.

Message and attachment size limitations are subject to the Google State enterprise account agreements.

E. Encryption: The Department utilizes e-mail encryption. Workforce members should use the word "encrypt" in the e-mail subject line to trigger message encryption when knowingly transmitting protected health information or personal identifying information (PHI or PII) outside of the Department via e-mail. *See* SOP PSP-032, Encryption of Workstation, Laptops, Email, and Mobile Computing Devices.

F. Prohibited Uses and Conduct: The following practices are prohibited:

1. Using the Department's computer systems, including e-mail, for personal profit or gain.

2. Using e-mail to send copies of documents and /or programs in violation of copyright laws.

3. Using e-mail to intimidate or threaten others.

4. Using e-mail in a manner that could be interpreted as racial or sexual harassment by any viewer.

5. Using e-mail communications to interfere with the ability of others to conduct official state business.

6. Sending or posting any messages or file containing a privileged work product, restricted data, or any otherwise confidential information, without appropriately marking the message or file.

7. Constructing an electronic message so it appears to be from someone else ("spoofing "). this does not preclude sending a message for another person at that person's request.

8. Forwarding a message after changing the text so it appears that the author has sent a different message.

9. Obtaining access to the files or messages of others absent proper authorization, substantial official state business purpose or need for systems maintenance.

10. Attempting unauthorized access to data or attempting to breach the Department security measures on any system or attempting to intercept any communications transmission without proper authorization.

11. Knowingly opening or running an executable attachment from a suspected virus contaminated e-mail message.

Violations of the policy stated above and/or engaging in prohibited conduct described here and may result in corrective or disciplinary action.

Workforce members are reminded that personal use of Departments computer systems, including e-mail capabilities, as with any state resource and equipment, may violate state statute, including but not limited to section 18-8-407, C.R.S and executive directives related to ethics. All workforce shall comply with the OIT Acceptable Use policy.

G. Email Signature Block: To maintain a consistent brand standard, the Department request that all workforce members utilize the 'New' and 'Replies ' Email Signature Block, and that workforce members not use emoticons (i.e. emojis or smiley faces), inspirational quotes, photographs or wallpaper images. All workforce members must add 'State Relay :711 'to their e-mail signature. Contact the Communications and Government Relations Division for templates that can be copied and pasted or consult SharePoint communications templates for current signature block standards.

V. Effective Date

This Standard Operating Procedure will become effective upon signature by the Executive Director and is effective until modified or terminated.

VIOLATION OF THIS STANDARD OPERATING PROCEDURE MAY RESULT IN CORRECTIVE OR DISCIPLINARY ACTION UP TO AND INCLUDING TERMINATION.

DocuSigned by:
Kim Bimestefer
0B6A84797EA8493...

SOP Effective Date[1]: 2/1/21

Authorizing Signature

[1] The format of this SOP was updated to ensure that it is accessible. This format update does not modify any requirements of the SOP and this SOP is still effective as written as of the SOP Effective Date shown.