Electronic Mail Policy

Effective Date	5/12/2009	DocuSigned by: Dr. Georgina Yoshioka 7DF8077EFA67482...
Revised Date	4/8/2025	Georgina Yoshioka, DSW, MBA, LCSW, Director

Policy

It is the policy of the Department of Behavioral Health (DBH), in partnership with the County's Innovation and Technology Department (ITD), to utilize Behavioral Health and/or County electronic mail (e-mail) systems as a means of communication for legitimate department business purposes and to ensure safeguarding of DBH client protected health information (PHI), when disclosing PHI electronically.

Purpose

The purpose of this policy is to provide instruction to the DBH workforce regarding appropriate use of e-mail in conducting department and county business, including safeguarding disclosure of client PHI. Staff shall carry out their duties while using e-mail in a professional and courteous manner and in accordance with Department and County policies.

Definitions

Breach: Acquisition, access, use or unauthorized disclosure of PHI in a manner not permitted under HIPAA, which compromises the security or privacy of the information. Impermissible use or disclosure is presumed to be a breach unless the covered entity demonstrates a low probability that the information has been compromised or if the disclosure falls under one of three exceptions as specified in 45 CFR §164.400-414.

Continued on next page

Definitions, continued

HIPAA identifiers: Elements in health data that are considered identifiers under the HIPAA safe harbor rule which must be removed prior to sharing client data, unless authorized by the client including:

1. Names;
2. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
   A. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
   B. The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. Telephone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Social security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images, and
18. Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c)

Note: Subsets of these elements are included as identifiers (e.g. initials, last 4 digits of social security number).

Internet: A worldwide, publicly accessible network of interconnected computer networks that transmit data.

Intranet: A privately maintained computer network that can be accessed only by authorized persons, such as members or employees of an organization.

Continued on next page

Definitions, continued

Personally Identifiable Information (PII): Information that can be used alone or in conjunction with other personal or identifying information, which is linked or linkable to a specific individual. This includes name, social security number, date of birth, address, driver's license, photo identification, other identifying number (case number, client index number, myAvatar number/medical record number, etc.).

Privacy/Security Incident: Any attempted or successful unauthorized access, use, disclosure, modification, or destruction of PHI or interference with operations in an information system that does not result in a breach.

Protected Health Information (PHI): Individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper or oral. Individually identifiable information is information, including demographic data, that relates to the individual's past, present or future physical or mental health or condition; the provision of health care to the individual; or the past, present, or future payment for the provision of health care to the individual, and identifies the individual or for which there is reasonable basis to believe it can be used to identify the individual. PHI excludes individually identifiable health information in education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; in records described at 20 U.S.C. 1232g(a)(4)(B)(iv); in employment records held by a covered entity in its role as employer; and regarding a person who has been deceased for more than fifty (50) years.

Privacy

Staff should have no expectation of privacy in any e-mail created, stored, sent or received on County e-mail systems. DBH and the County reserve the right to monitor, access, copy or delete any messages stored in its e-mail systems without advance notice to staff.

Staff is expected to respect the privacy of e-mail messages sent to others using the County's e-mail systems. Unless staff are authorized to do so, employees are prohibited from performing the following acts to another employee's information or e-mail without that employee's permission:

- Accessing
- Viewing
- Retrieving
- Listening to
- Tampering with
- Copying
- Changing
- Printing
- Deleting
- Composing messages

Personal use of DBH E-mail

Limited, occasional or incidental use of the e-mail system for personal purposes may be acceptable, if done in a professional and appropriate manner as follows:

- Not on County time;
- Not violating prohibited activities contained in this policy;
- Not interfering with the conduct of County business or the performance of the employee's duties.

E-mail messages sent using the County e-mail system for personal purposes shall be treated as business messages and may become public records in accordance with the Public Records Act.

Sending & Receiving PHI/PII

Internal Network E-mail Communications:
Internal County e-mail (sbcounty.gov) communication is routed through an internal network. This network can be used to communicate PHI or PII when necessary for the completion of job duties within the following guidelines:

- Addresses should be confirmed before sending to ensure the e-mail is delivered to the appropriate recipient, and
- The minimum necessary amount of PHI or PII should be included in the e-mail to accomplish the intended purpose.
- The only client information the signature line may include is the client initials along with *"Confidential."*

External Network E-mail Communications:
All e-mails sent outside of the County Network transmitting *Sensitive or Highly Sensitive* information including client PII/PHI **must** be encrypted to meet requirements of the HIPAA Security Rule (164.312(a)(1) and 164.312(e)(1).

- Sensitive and Highly Sensitive information may be sent via e-mail provided the sender adheres to the following guidelines:
  - Addresses shall be confirmed before sending to ensure the e-mail is delivered to the appropriate recipient.
  - The minimum necessary amount of PHI shall be included in the e-mail to accomplish the intended purpose.
  - Encryption mechanism is confirmed prior to transmission.

Receiving E-mailed PHI/PII
Any workforce member who receives an unencrypted e-mail containing PHI/PII from outside the County's network, must report the e-mail as a possible breach or security incident to the DBH Office of Compliance in accordance with the Privacy Incident Policy (COM0944).

Continued on next page

Sending & Receiving PHI/PII, continued

Unintended Recipient(s)

In the event an e-mail containing client information may have been inadvertently delivered to the wrong recipient (for example, due to an incorrect e-mail address), recall of the e-mail is to be immediately initiated and notification made to the DBH Office of Compliance.

Prohibited Activities

It is a violation of this policy to use e-mail to violate existing law, regulation, County or department policy, the Code of Conduct or County Personnel Rules. Other prohibited uses of the County e-mail systems include, but are limited to:

- Activity that could expose the County to civil or criminal liability;
- Sending Protected Health Information (PHI) and/or Personally Identifiable Information (PII) in the body of or an attachment to an e-mail outside the County network that does not meet a minimum of 256-Bit encryption;
- Sending PII retrieved from the Medi-Cal Eligibility Data System (MEDS) in the body of or an attachment to an e-mail that does not meet the minimum of 256-Bit encryption;
- Representing oneself as a spokesperson and/or making commitments on behalf of the County or a department without authorization;
- Use intended for personal or commercial financial gain or participating in any gaming, wagering or gaming activities
- Any use of e-mail for the purpose of distributing materials, promoting causes or beliefs or soliciting membership in, support for, or donations to any organization, group or entity including, but not limited to, those of a commercial, political, charitable or ideological nature unless officially sanctioned by the County;
- Use of e-mail to prepare, solicit, distribute or transmit offensive, abusive, threatening, pornographic, sexually explicit or hate messages or images;
- Utilization of e-mail to prepare, solicit, distribute or transmit obscene, offensive, harassing, derogatory, or disparaging comments, jokes or slurs related to race, color, ethnicity, gender, age, sex, religion, disability or political affiliation;
- Use of e-mail to commit illegal, fraudulent or malicious activities;
- Originating or intentionally propagating computer viruses and/or chain letters or petitions;
- Disclosing confidential and/or personal information without appropriate authorization or sharing County e-mail accounts or passwords to access those accounts with others; Personal use that results in any charges or other costs to the County;

Continued on next page

Prohibited Activities, continued

- Subscribing to external mailing lists, notification services or other e-mail services not reasonably related to the performance of assigned job duties, or
- Using animation, specialized graphics, stationary or color backgrounds in e-mails.

Employees who receive e-mail with content they feel violates these policies should report the matter to their supervisor immediately or to the DBH-IT Helpdesk.

***Note**:* County and departmental policies prohibiting sexual and other harassment are applicable to the use of the County's e-mail systems.

Unsolicited E-mails

As a result of e-mail systems becoming a primary means of distributing computer malware, SPAM, and phishing attempts, the County has taken appropriate actions to filter and to relieve the e-mail system of unsolicited e-mails as well as to restrict incoming e-mail to protect the County's computer systems.

Workforce members shall treat all unsolicited e-mails with suspicion, particularly e-mails received from the Internet (i.e. non-County e-mail addresses) or those e-mails requesting the workforce member's log-in information and passwords. Questions regarding the authenticity and integrity of an e-mail should be referred (forwarded as an attachment) to the DBH-IT Security team at DBH-ITSecurity@dbh.sbcounty.gov so that it can be reviewed and/or deleted from the workforce member's account.

E-mail Signatures

All DBH staff e-mails will have the County-branded signature banner, which includes the required confidentiality notice. The e-mail signature shall not include personal details, quotations, or graphics that are unrelated to County business.

Attorney-Client Privileged Communication

E-mails between DBH, County Counsel and/or its outside attorney(s) constitute confidential and privileged communication. The content of the e-mail(s) cannot be forwarded without authorization of counsel.

E-mail Broadcasts

E-mail shall not be used to announce, advertise or otherwise promulgate any event, cause, organization or activity that is not an official County of San Bernardino or Department of Behavioral Health function or program. Any use of the e-mail system to promulgate a legitimate event countywide or department wide must be approved by the DBH Public Information Officer and comply with the DBH Web Blast Policy.

Microsoft 365 Message Encryption

San Bernardino County DBH utilizes Microsoft 365 Message Encryption to secure its e-mail communications. This service allows DBH to send encrypted messages via e-mail. The encrypted e-mail can only be opened by authorized recipients who authenticate themselves and must be used on all e-mails containing client PHI when leaving the County Network.

Sending an Encrypted E-mail

Employees may only send e-mails containing protected health information (PHI), outside of the network if there is 256-bit encryption, at minimum or by an acceptable encryption method designated by ITD. Please be advised Microsoft 365 Message Encryption is the acceptable encryption method designated by ITD.

Staff are reminded that sending PHI to personal devices or e-mail addresses is not allowed even if the PHI is encrypted as DBH staff may only access PHI remotely using County issued equipment.

Prior to sending an e-mail containing PHI, DBH employees shall:

- Determine if the best method of communication is e-mail;
- Determine whether the e-mail recipient is entitled to receive the PHI (either as permitted by law or based on authorization from the client);
- Ensure PHI is sent as an attachment rather than in the body of the email;
- Confirm recipient's e-mail address to ensure PHI is not misdirected,
- Confirm there is no PHI or client identifiers included in the subject line of the email, and
- Limit PHI in the body of the email to the minimum necessary.

Note: Do not forward strings of emails containing PHI, prepare a new message with only the minimum necessary information.

Continued on next page

Electronic Mail Policy, Continued

Sending an Encrypted E-mail, continued

To encrypt an e-mail leaving the County's network, staff must preface the subject line with the following phrase: PHI: or phi:

Important Note: Please note the letters are not case sensitive and there are not any spacing requirements after the colon. Senders can use one (1) or two (2) spaces after the colon before documenting the e-mail subject line for encryption to be enabled.

Example of proper formatting:

DBH staff may send encrypted e-mail from their County issued mobile devices such as smart phones and tablets or via webmail. Staff is reminded that accessing e-mail through webmail is only allowed while staff is conducting County business.

Notification to Encrypted E-mail Recipient

Prior to sending an encrypted e-mail to a first-time recipient, DBH staff should send the recipient notification that the person will receive an encrypted e-mail from DBH along with the instructions detailed in the next section.

Important Note: Do not send the e-mail registration instructions in the same e-mail as the encrypted message.

E-Mail Recipient Responsibility

E-mail recipients must follow the steps indicated in the encrypted e-mail. Once the recipient has been authenticated, the person will only be required to enter a password thereafter to open and view secure e-mail from DBH.

Step	Action
1	Upon receipt of encrypted e-mail, recipient will need to click the **Read the Message** button
2	A new tab will open - Recipient will click the **Sign in with a One-time passcode** button
3	Recipient will receive a passcode in their e-mail • Sender is: **Microsoft Office 365 Message Encryption**
4	Recipient will need to enter the passcode and select Continue
5	Recipient can now access the encrypted message in the e-mail

---

Secure E-Mail Recipient's Workflow Process

The following workflow depicts the process e-mail recipients complete when receiving an encrypted e-mail from DBH.

Encryption Methods

It is the responsibility of the Innovation and Technology Department (ITD) to determine what encryption methods are acceptable and provide guidance on the implementation and use of the approved methods. Any difficulties or questions regarding this process should be directed to the DBH Helpdesk at (909) 386-9730.

Related Policy or Procedure

County of San Bernardino Policy Manual

- 09-01: Electronic Mail (E-mail) Systems
- 09-04: Internet/Intranet Use Policy
- 14-02: Non-Public Personally Identifiable Information
- 14-04: Internet/Intranet Use
- 16-02: Protection of Individually Identifiable Health Information

DBH Standard Practice Manual

- COM0944: Privacy Incident Policy
- IT5003: Internet Account Policy
- IT5004: Computer and Network Appropriate Use Policy
- IT5006: Remote Access Policy
- IT5008: Device and Media Controls Policy
- IT5009: User I.D. and Password Policy

Reference(s)

California Civil Code 56 et seq. (The Confidentiality of Medical Information Act)

Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, Privacy Rule (HIPAA)
