

# Black Hawk County Public Health

## Policy Statement

<b>TITLE:</b> Electronic Communications Policy		<b>STATUS:</b> <div><input type="checkbox"/> Review Only <input type="checkbox"/> Draft <input type="checkbox"/> Pending Approval <input checked="" type="checkbox"/> Approved</div>		<b>PAGE</b> 1 of 12
<b>EFFECTIVE DATE:</b>	01/29/2025	<b>LATEST REVISION/REVIEW:</b>	01/2025	
<b>NEXT REVIEW DATE:</b>	10/2025	<b>ORIGINATION DATE:</b>	04/27/2022	
<b>PUBLIC HEALTH DIRECTOR APPROVAL:</b>	01/2025	<b>BOARD OF HEALTH APPROVAL:</b>	01/29/2025	
<b>REVIEW/REVISION HISTORY (MM/DD/YYYY):</b> New Policy, 04/27/2022; 10/17/2023 ,01/2024, 01/2025				

**PURPOSE:** It is the policy of Black Hawk County Public Health (BHCPH) that all interactions by employees, interns, or volunteers, through electronic communications and social media, both professionally and personally, are conducted in a professional and responsible manner consistent with county and health department policy. This document provides guidance and addresses security risks and procedural issues presented by use of technology for communication of public health-related information and activities.

**SCOPE:** This policy is applicable to all Black Hawk County Public Health (BHCPH) employees. Whenever the provisions of this policy conflict with federal, state, or local laws or regulations, or with a current collective bargaining agreement between the County and a certified bargaining unit, the provisions of the collective bargaining agreement and/or the laws or regulations shall prevail.

### DEFINITIONS:

**Electronic Communications (e-communications):** any communication created, sent, forwarded, replied to, transmitted, stored, copied, downloaded, displayed, viewed, or read/received by means of electronic networks or computer systems, which may include, but is not limited to email (using county-issued email Outlook accounts only), text (SMS, MMS) messaging, iMessages, instant messaging, push notifications, file transfer, cloud services, social networking, blogging, electronic bulletin boards, listservs, and newsgroups.

**Social Media/Social Network:** broadly understood for purposes of this policy to include blogs, wikis, microblogs, message boards, electronic newsletters, online journals, online forums, online collaborative information, and publishing systems that are accessible to internal and external audiences, video sharing (e.g., YouTube) social networking sites and applications, and other sites and services that permit users to share information with others in a contemporaneous manner. This policy is meant to address social media in general. Advances in technology and new social media tools will emerge that are expected to be used in accordance with this policy.

**SMS (Short Message Service or Text Messaging):** The sending of 160-character messages over a cell phone or through a web-based interface to one or more cellphone recipients.

**Multimedia Messaging Service (MMS):** a system that enables mobile devices to send and receive digital images, pictures, videos, and sound content, as well as text messages with extended character limits.

**iMessages:** texts, photos, or videos that are sent to another iOS device.

**Short Code:** Five- or six-digit special telephone numbers used for sending SMS messages.

**Push Notifications:** a message that appears as a pop-up on a recipient's device, allowing the recipient to take a specific action or opt-in to timely updates. Typically formatted as text and rich media (e.g., images and buttons).

**Protected Health Information (PHI):** Individually identifiable health information in any form whether oral, written or electronic. Individually identifiable health information refers to information 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.
- Identifies the individual, or for which there is a reasonable basis to believe it can be used to identify the individual.

**Electronic Protected Health Information (ePHI):** Protected health information that is transmitted or maintained in electronic media.

**Subscriber or Public:** Individuals who can opt in to receive general educational health promotion and prevention messages.

**Client:** A member of the public who presents, or has presented, for health care, including minors and adults receiving health care, informing or care coordination services, dental services, and other health care services from BHCPH care sites and/or programs. Clients include those who have been identified as a case or contact during disease surveillance and investigation activities, as well as deceased persons who have received care.

**Black Hawk County Public Health Information:** Information in any form or media that is created by or on behalf of BHCPH in the course and scope of its business, regardless of whether that information is maintained or stored by BHCPH or others on behalf of BHCPH. Examples of BHCPH information include, but are not limited to, client records, personnel records, financial information, company competitive information, and business e-mail messages.

---

## **POLICY LANGUAGE:**

All electronic communications of confidential data must be encrypted using only BHC-approved electronic communication services and encryption technologies unless written consent is provided by a recipient who requests the use of unencrypted communication and acknowledges the risk of a third-party viewing the communication. Confidential data may not be shared on or posted to social networking sites, blogs, electronic bulletin boards, listservs, newsgroups, or another public electronic forum. Electronic communication of confidential data shall be limited to the minimum necessary to accomplish the purpose of the disclosure. There is an exception to minimum necessary when the disclosure is for treatment or public health surveillance and investigation purposes. Email communication of PHI will be consistent with these requirements.

### ***Internet-based Partner Services***

Per Iowa Code, Black Hawk County Public Health (BHCPH) is required to conduct disease surveillance and investigation activities for reportable diseases. Under contract with the Iowa Health and Human Services(Iowa HHS), BHCPH must maintain enhanced investigative and outreach tools for searching and private/direct messaging on common social networking sites and apps for disease investigation activities. As such, BHCPH adopts the current *Iowa Department of Public Health Internet-based Partner Services Policy Document* (undated), attached hereto. During BHCPH's annual policy review, or upon earlier notification of updates by Iowa HHS, BHCPH will verify it has the most current Iowa HHS internet-based partner services policy document.

Due to the constantly evolving nature of technology, all available social media and e-communications platforms are not specified in this policy but may include encrypted county-issued and monitored email accounts (Outlook accounts only; Gmail is not an allowable platform), Meta (f/k/a Facebook), Messenger from Meta (f/k/a Facebook Messenger), Snapchat, Instagram, Tinder, Grindr, and WhatsApp. Regardless of the platform, all user accounts and related desktop or mobile applications require approval from the public health director or designee. A record of user accounts will be maintained to document the user accounts on each platform, and the associated usernames and staff members. All user accounts must be connected to a Black Hawk County-issued email address, and the recovery information for each account must be connected back to department phone numbers and email addresses. User accounts may not be connected to staff personal accounts, personal email, or personal phone numbers. User accounts may only be accessed from department-issued devices.

BHCPH will coordinate with the information technology department and county privacy and/or security officer to ensure appropriate approval for use, and implementation/monitoring of the platform or resource for HIPAA policy and procedure compliance. Staff must make their user accounts available to their supervisor or county privacy and/or security officer upon request for the purpose of oversight, audit, and review for appropriate use. Failure to make a user account available for review, or misuse of a user account, may result in disciplinary action.

Certain public health-related activities, such as disease surveillance, investigation, and/or intervention activities, are an exception to the HIPAA Privacy disclosure requirements. As such, a release of information is not required to be obtained prior to performing those activities. Additionally, written and/or verbal consent for communication is not required prior to attempting to contact an individual at risk of contracting or spreading a disease or condition.

Per Iowa Code Section 139A.35, a minor shall have the legal capacity to act and give consent to provision of medical care or services to the minor for the prevention, diagnosis, or treatment of a sexually transmitted disease or infection by a hospital, clinic, or health care provider.

---

### ***Social Media Communications*** (supplemental guidelines to the Black Hawk County Social Media Policy)

The social media accounts of Black Hawk County Public Health (BHCPH) are maintained for the purpose of disseminating public health information. BHCPH makes every effort to ensure the accuracy of the information provided on its social networking pages. However, several factors that are beyond the County's control (including public comments, unauthorized modification of electronic data, transmission errors, browser incompatibilities, information that has been cached on the local computer or storage device, or other aspects of electronic communication) can affect the quality of the information displayed on the County's associated sites. For that reason, BHCPH does not guarantee the accuracy of the information provided on its social networking sites and is not liable for reliance on this information.

Accessibility: Every effort will be made to reduce barriers of accessing public health information promoted on BHCPH's social media accounts. The Communications team will provide information that considers culture, language, literacy, and varied abilities to access information. The team will seek social media channels that reach a wide audience and utilize guidance that increases the accessibility of content for all abilities.

Privacy: All content posted on these accounts is public record and is subject to public disclosure. The primary purpose of this page is to provide up-to-date public health information and services to the community, but the ability to post comments serves as a limited public forum for constituents to respond or react to that information, which constitutes government speech.

Submission of public questions, comments, and concerns is allowed and encouraged; however, BHCPH will monitor such submissions during regular business hours.

These accounts are actively moderated and may be subject to social media platform Community Standards. Certain types of posts or comments are not considered protected forms of speech and may be subject to removal by BHCPH.

### Public Information Officer Responsibility:

- A. The Public Information Officer (PIO) is responsible for all agency social media pages, feeds, and platforms. Information Technology (IT) will assist the PIO and Communications team with developing future opportunities to effectively use live internet-based communication.
- B. Should the PIO or person(s) designated to social media activities or accounts leave the agency, passwords will be changed.

- C. Only the PIO, or designee, may send messages and/or respond to comments via agency social media platforms and create new pages, feeds, groups, etc., on social networks. The PIO will have the final say on selection of new social media tools, with consultation from IT. IT carries responsibility for technical and security issues.

Standard Practices:

- A. Any individual designated to the agency's social media accounts will follow these practices:
1. Protect sensitive or personally identifying information.
  2. Monitor user comments (if enabled).
    - a. If a user submits a negative comment, the PIO should be notified promptly. No agency personnel with access to BHCPH's social media accounts shall respond to negative or aggrieved comments unless granted by the Public Health Director or PIO.
  3. Maintain information accuracy.
  4. Correct identified mistakes.
  5. Be considerate.
  6. Respect copyrights and trademarks.
  7. User county-issued and monitored email accounts and strong passwords (e.g., alpha-numeric, upper and lower case, symbols, etc.).
  8. Avoid advertisements, sponsorships, and endorsements.
  9. Stay within area of expertise.
  10. Stay within scope of agency's role.
  11. Avoid use for political purposes.

Content Management:

- A. Only content related to agency programs and available services will be distributed via the agency's social media channels. Examples include:
1. Announcements and discussions related to upcoming events, such as training programs, available services, workshops, and awareness displays.
  2. Media releases.
  3. Links to videos explaining agency programs.
  4. Repurposed content distributed and provided from trusted sources/partners that are relevant to public health topics and information. Examples or sources are listed in the *Black Hawk County Public Health Communications Plan*.

Branding: All agency social media accounts will have a consistent look and feel, including use of the agency's logo. Consult the *Black Hawk County Brand Style Guide* standard operating procedure for more information.

Implied Endorsements: If possible, the agency's content will not appear next to advertisements or used in such a way that implies approval or support for all-encompassing material without prior approval from the PIO.

Monitoring: The PIO, or designee, shall closely monitor social media. He/she will view agency social media networking pages at least once each weekday and periodically on weekends. The PIO, or designee, will respond to social media inquiries within a reasonable amount of time.

Public Records: Social media users should be aware that any type of communication on social media may be used as a public record. No expectation of privacy arises from the use of agency information systems or social media sites which officially represent the agency. The agency reserves the right to monitor the use of agency information systems and hardware with or without notice.

Common Practice Guidelines:

- A. The following statement is posted to all agency social media pages for which commenting is available:
1. "We welcome you and your comments to Black Hawk County Public Health [enter social media source] page."
- B. Once posted, BHCPH reserves the right to delete submissions that:

1. Contain vulgar language, personal attacks of any kind, offensive and derogatory comments, or other language that promotes bias against others as outlined in the Black Hawk County Board of Health "[Bias is a Public Health Crisis](#)" position statement.
  2. Are spam or include links to other sites.
  3. Are clearly off-topic.
  4. Advocate illegal activity.
  5. Promote particular services, products, or political organizations.
  6. Infringe on copyrights or trademarks.
  7. Use personally identifiable information.
  8. Contain client-specific and other confidential information.
- C. The Electronics Communication SOP outlines the process for removing comments from social media platforms. When a comment is removed, BHCPH will post a reason for removing the comment (e.g., "A comment to this post was removed because it violated BHCPH Common Practice Guidelines.")
- D. BHCPH reserves the right to restrict or remove any content that is deemed in violation of this policy or any applicable law, consulting with the Black Hawk Assistant County Attorney as needed. Any content that is removed based on this policy, or applicable laws, will be documented on the Content Removal Tracking Form attached hereto. The completed form will be submitted to the department's PIO. The PIO will retain the removed content in accordance with the county's policy on retention of such information.
- E. Banning people: If there are any violations of the comments policy above, then BHCPH reserves the right to ban participation on platforms that permit organizations to ban users.
- F. Platform rules: Please note that social media platforms have their own rules of conduct, or Community Standards, so social media platforms may take their own action to remove comments or ban users. BHCPH is not responsible for those actions.
- G. Video disclaimer: BHCPH is not responsible for the content provided on "related" and "promoted" videos that are accessible from social media video channels. All viewers should note that these related videos and comments expressed on them do not necessarily reflect the opinions and position of the BHCPH or its officers and employees. Videos that violate the social media platform's Community Standards or guidelines outlined above, will be removed.
- H. Archiving: All posts and comments are archived.
- I. Private messages: Many social media platforms provide a non-public way to contact BHCPH social media accounts, however, those conversations are public records and subject to Iowa Freedom of Information Act requests.
- J. Redress process: If a person thinks BHCPH acted wrongfully regarding the removal of comments or participation on BHCPH social media accounts, they may petition BHCPH for review by contacting [compliance@blackhawkcounty.iowa.gov](mailto:compliance@blackhawkcounty.iowa.gov).
- K. Questions regarding the BHCPH Electronic Communications policy can be emailed to [publichealth@blackhawkcounty.iowa.gov](mailto:publichealth@blackhawkcounty.iowa.gov).

#### Guidelines for Individual Use:

- A. Employees are expected to adhere to BHCPH's policies when using or participating in social media. All rules that apply to other BHCPH communications apply here, including confidentiality, e-mail and internet use, photography and video, and media relations.
- B. If authorized, employees may use social media during work hours for business-related reasons only. Property of BHCPH, including computers, online tools, and web access, will be provided for authorized work purposes. Personal use of social media will be limited to break or meal periods only, using personally owned devices.

- C. Employees shall not post any material that is obscene, defamatory, profane, libelous, threatening, harassing, abusive, hateful, or embarrassing to another person or entity when posting to BHCPH-hosted sites.
- D. Employees shall not post content or conduct any activity that fails to conform to any and all applicable state, federal, or local laws. For BHCPH's and our employees' protection, it is critical that everyone abide by copyright laws by ensuring that they have permission to use or reproduce any copyrighted text, photos, graphics, video, or other material owned by others.
- E. Employees shall seek approval in writing from the PIO before setting up a BHCPH-affiliated online journal or other social media site.
- F. Employees shall not use or disclose any client-identifiable information of any kind on any social media without the express written permission of the client and prior approval from the PIO. Even if an individual is not identified by name, if there is a reasonable basis to believe that the person could still be identified from that information, this could constitute a violation of the Health Insurance Portability and Accountability Act (HIPAA) and BHCPH policy.

Disclosure of Employment on Social Media:

- A. Proprietary Information: Employees may not disclose any confidential or proprietary information of or about BHCPH, its affiliates, vendors, or suppliers, including but not limited to, business and financial information; represent that they are communicating the views of BHCPH; or do anything that might reasonably create the impression that they are communicating on behalf of, or as a representative of, BHCPH.
- B. Self-hosted sites:
  - 1. Employees must refrain from saying or suggesting that the views and opinions they express related to BHCPH or health care topics represent the official views of BHCPH.
  - 2. Write in the first person: where a connection to BHCPH is apparent, a BHCPH employee must make it clear that they are speaking for themselves, and not on behalf of BHCPH. The following disclaimer is to be used:

“The views expressed on this [online journal or social media website] are my own and do not reflect the views of my employer.” This language should be added to the “About me” (or similarly available) section of an online journal or social networking profile where employment with BHCPH is identified, known, or presumed.
  - 3. Take responsibility: employees are personally responsible for the content on their social media sites and/or online journals. Employees will be mindful that what is written will be public for a long time.
  - 4. Respect BHCPH's brand and reputation: if an employee's online journal, social media posts or comments, or other online activities are inconsistent with, or would negatively impact, BHCPH's reputation or brand, the employee shall not refer to BHCPH or identify BHCPH as the employee's employer. Each employee has a choice whether to disclose their employment status with BHCPH through social media. Employees who choose to disclose their employment with BHCPH when using social media are required to adhere to all applicable policies and procedures, including this policy.
  - 5. Coordinate business-related social media: some BHCPH staff members may be interested in engaging in internet conversations for work-related purposes or may be asked by supervisors or leadership to participate, in support of BHCPH organizational objectives. Such engagement on behalf of BHCPH must be pre-approved in writing and coordinated through the supervisor or the PIO.
- C. Employee conduct on social media: whether in a professional or personal capacity, that adversely affects job performance, the performance of fellow co-workers, or otherwise affects the public, may result in disciplinary action up to and including termination.

1. Employees are expected to adhere to the Health Department's *Ethics Policy*, *Black Hawk County Social Media Policy*; *Black Hawk County Work Rules Policy*; *Black Hawk County Computer, Internet and Email Usage Policy*; *Black Hawk County Discrimination/Harassment and Retaliation policy*; *Black Hawk County Workplace Violence Policy*; *Black Hawk County Policies and Procedures for Compliance with the Health Insurance Portability and Accountability Act of 1996 "HIPAA," Record Retention Policy*, and all other applicable BHCPH policies and procedures.
2. Inappropriate postings regarding co-workers, supervisors, or BHCPH that are vulgar, obscene, or include discriminatory remarks, harassment, intimidation, threats of violence or similar inappropriate or unlawful conduct, or are otherwise in violation of the policies mentioned above, will not be tolerated and may subject employees to disciplinary action up to and including termination.
3. Health department policies, with respect to these prohibitions, apply to both off-duty (non-working hours) and on-duty (working hours) conduct.

---

### ***Messaging and Electronic Mail***

The HIPAA Privacy Rule not only allows, but requires, covered entities to communicate with patients via email or messaging if requested in writing by the patient, and with reasonable safeguards in place when doing so. It is the policy of the BHCPH to permit the limited use of messaging to communicate with the public or clients in a manner that is consistent with the HIPAA Security Rule. To satisfy the HIPAA Security Rule, messages must be structured to remove PHI and retain limited personal health information in the message, or a risk analysis must be completed.

If the network or means of communication is not secure and/or the PHI/e-PHI is not encrypted, the department may still communicate with patients via email or messaging, so long as the patient is warned of the risk in advance and the individual maintains a preference for use of the unencrypted method of communication. The department's obligation is to notify the individual that there may be some level of risk that the information could be read by a third party.

Internal Notice of Messaging Program: Prior to implementing a new messaging program, and periodically, a risk assessment must be completed by the departmental HIPAA liaison, in coordination with the HIPAA Privacy and Security officers, to ensure compliance with the HIPAA Security Rule.

Program Managers, the Public Health Communications Strategist, or Public Health Planner will consult and inform the BHCPH HIPAA liaison prior to launching a messaging program using, but not limited to, SMS, MMS, iMessage, push notifications, or private/direct messaging. The liaison will provide logistical assistance and messaging guidance and support in consultation with BHC Privacy and Security Officers and Assistant County Attorney.

Approved Devices for Sending Messages: messages must be sent from devices owned or approved by Black Hawk County, or from an approved computer application.

### **Public Records:**

- A. Public records requests related to messaging should be forwarded to the Black Hawk Assistant County Attorney for a decision about whether the requested records may be released.
- B. On request, the agency will provide access to, or copies of, messaging records that are subject to public access under Iowa's public records law.
- C. BHCPH will not provide access to, or copies of, records containing PHI/ePHI, as those records are excepted from public access.

***Note: The public has a right to access and obtain a copy of records created by government agencies transacting agency business unless an exception applies. However, there is no exception that***

***applies generally to messages that do not contain PHI. There is also no exception that applies generally to the telephone numbers of member of the public who subscribe to messages, but it is possible that another exception may apply to protect an individual phone number.***

Message Retention: messages should be deleted from mobile devices but must be retained elsewhere if required by applicable records retention requirements. A record of the communication must be documented in the applicable database/information system used for documenting client-related activities. While the message content does not need to be documented verbatim, the occurrence must be documented.

Opt-in/Consent Requirement: To receive messages through an application/program or messaging platform covered by this policy, a subscriber or client must opt-in or consent.

- A. A subscriber or client may opt in or consent to receive general public health messages or specific health-related messages (e.g., appointment reminders) by signing a written opt-in form, using a website form, or using a short code.
- B. The opt-in method must provide the following information:
  - 1. A statement that the subscriber's cellular service provider may charge the subscriber a fee for transmitting and delivering messages. Agency staff should be aware that some people may be charged for messages by their phone service providers and that messages exceeding 160 characters will be sent as two or more messages. Staff will be judicious in the length of messages and in the number of messages sent.
  - 2. Instructions for how to opt-out of receiving messages.
  - 3. A request that the subscriber notify BHCPH of a change in phone number, and information about how to provide that information.
  - 4. That unencrypted messaging comes with a risk and may be read by a third party.
- C. Permission is voluntary and clients are under no obligation to receive BHCPH electronic communications. Clients who do not wish to receive notices or message may "opt-out" from receiving electronic messages at any time by notifying BHCPH by phone or in writing. Opting out is effective from that date forward, and not retroactively. If a client informs an employee of his/her desire to opt out, it is that employee's responsibility to notify the appropriate staff to deactivate the client from electronic messaging.
- D. Opt-out information should be sent to subscribers of messaging programs (e.g., NotifyMe) periodically to remind them how to unsubscribe from messaging.
- E. Certain public health-related activities, such as disease surveillance, investigation, and/or interventions activities, are an exception to the HIPAA Privacy disclosure requirements. As such, a release of information is not required to be obtained prior to performing those activities. Additionally, written and/or verbal consent for communication may not be possible, and is not required, prior to attempting to contact an individual at risk of contracting or spreading a disease or condition.

Messages Must Not Contain PHI: messages sent through a messaging program (e.g. NotifyMe) to subscribers must not contain protected health information. This section pertains to public health messaging that is not related to direct care services or part of a program area that routinely deals with client-specific health-related information, such as disease surveillance and investigation, chronic disease prevention, healthy homes, etc.

Security Risk Analysis: A security risk analysis is required when new methods of storing or transmitting ePHI, such as messaging, are adopted. This requires a covered entity to identify where and how it acquires, creates, or maintains ePHI; assess its current security measures; identify threats to the security of ePHI; and determine the likelihood of those threats occurring. In coordination with BHC Privacy and Security Officer, BHCPH will conduct a security risk analysis before implementing a program to send messages.

Administrative, Physical, and Technical Safeguards:



- A. BHCPH will identify which devices or computer applications may be used for sending messages. No other devices or applications may be used.
- B. Agency staff should assure that client cell phone numbers are recorded accurately and should periodically verify the number with the client.
- C. If a mobile device is used for messaging, staff members must:
  - 1. Comply with existing policies for securing mobile devices that are used to access or transmit ePHI, including assuring the mobile device used to send messages is always secure while at work and offsite (if permissible).
  - 2. Utilize passcode or biometric security safeguards.
  - 3. Delete the messages after the communication is completed and necessary information is recorded.
- D. Full client names must not be stored in the address books or contacts lists of mobile devices. First name and last initial is permissible.
- E. Limit or exclude, where possible, client identifiers when sending a message. Never use first and last name in a message.
- F. If a third-party vendor will be used to send messages, the departmental HIPAA liaison must be consulted first to assure an appropriate system is selected and security controls are thoroughly evaluated.

Message Content: Messages must be limited to the following information:

- Sender first name (optional)
- Agency name
- Client first name
- Telephone number for client to call with questions or for other information pertaining to the message.

Responding to Messages Received from Subscribers or Clients:

BHCPH may respond to messages received from subscribers to public health messages. If a message containing PHI is received, the staff member should respond only with a brief messaging asking the person to call the staff member or another appropriate person in the department.

BHCPH will respond to messages generated by health care clients (whether direct care or as part of a program area that routinely deals with client-specific health-related information, such as disease surveillance and investigation, chronic disease prevention, healthy homes, etc.) with a message asking the client to call. The response should include the first name and phone number of the appropriate person to call.

Messages received from subscribers or clients will be deleted from mobile devices after necessary information is documented in accordance with programmatic or records retention policies.

If a staff member receives a work-related message on a personal device or account, the staff member will use a county-owned device and business account to provide the sender with the appropriate BHCPH contact information for future communications.

Other Uses of Messaging by BHCPH Staff:

BHCPH recognizes that agency staff may use messaging in ways other than those addressed by this policy. Agency staff who use messages in the transaction of agency business for purposes not covered by this policy must comply with the following:

- A. Messages must not include PHI or other confidential information.
- B. Retain messages if retention is required by BHCPH or Iowa records retention schedules
- C. On request, provide members of the public access to or copies of messages, unless an exception to the

Public Records Law applies. Public records requests for a staff member's messages should be forwarded to the Black Hawk Assistant County Attorney for management.

Responsibilities:

- A. BHCPH HIPAA liaison or designee is responsible for documenting messaging exceptions throughout BHCPH.
- B. Program Managers or Supervisors are responsible for ensuring public health workforce follows messaging best practices and policies.
- C. The HIPAA liaison or designee is responsible for providing guidance to programs on messaging best practices.
- D. The Public Health Director or designee is responsible for approval of Electronic Communications policy exceptions.

Maintenance:

- A. Review
  - 1. This policy is to be reviewed annually to ensure compliance with applicable agency or accreditation standards, agreements, laws, or regulations.
  - 2. This policy may be reviewed more frequently as appropriate.
- B. Revision
  - 1. All changes made to this policy are to be noted on the **Record of Change** attached hereto.
  - 2. Substantial changes will require renewed Board of Health approval. This includes changes to the purpose, scope, or policy language.
  - 3. Changes in style, format, grammar, or minor error correction will not require renewed Board of Health approval but must be indicated on the Record of Change.

---

**RELATED RESOURCES:**

- A. Policies:** Black Hawk County Social Media Policy; Black Hawk County Work Rules Policy; Black Hawk County Computer, Internet, and Email Usage Policy; Black Hawk County Discrimination/Harassment and Retaliation policy; Black Hawk County Workplace Violence Policy; Black Hawk County Policies and Procedures for Compliance with the Health Insurance Portability and Accountability Act of 1996 "HIPAA"; other applicable BHC policies and procedures;
- B. Procedures:** Mobile Device Application Approval and Purchase, Electronic Communications SOP
- C. Forms:** Content Removal Tracking Form;
- D. Guidelines:** Accessibility Guidelines; Black Hawk County Public Health Communication Plan; BHCPH Brand Guidelines
- E. Legislation:** HIPAA Privacy & Security Rules, including Disclosures for Public Health Activities; Iowa Code Section 139A.35 (Minors)
- F. Other Documents:**
- G. Attachments:** Iowa Department of Public Health Internet-based Partner Services Policy Document (undated)

## Content Removal Tracking Form

### Archive Removal of Information from Social Media Sites

Today's Date:
Date comment was posted:
Date comment was removed:
Original post (link to screen shot)
Social Media Platform
Post ID (if available)
What was removed
Username
Link to user social media profile:
Link to screenshot of removed content
Reason for removing the comment:
Staff who removed

## Record of Change (Required for all policies)

Date of Change	Changes Made By	Changes Made/Notes	Approved By
04/27/2022	Megan Olmstead	Removed the word repeated on pg. 5, Common Practice, Letter E, Banning People, to understand that any violations not just repeated violations can be considered for banning people	Board of Health-voted on new policy with this change request
10/17/2023	Gabbi DeWitt	To adhere with brand guidelines, document was updated from Black Hawk County Health Department (BHCHD) to Black Hawk County Public Health (BHCPH) and font was updated from Times New Roman to Arial.	Policy Committee, BOH
10/17/2023	Gabbi DeWitt	Revised language on p. 4 to include BOH Bias Statement  Previously: Contain vulgar language, personal attacks of any kind, or other offensive and derogatory comments based on religion, race, ethnicity, sex, or disability.  Updated: Contain vulgar language, personal attacks of any kind, offensive and derogatory comments, or other language that promotes bias against others as outlined in the Black Hawk County Board of Health " <a href="#">Bias is a Public Health Crisis</a> " position statement.	Policy Committee, BOH
10/17/2023	Gabbi DeWitt	P4 - changed Common Practice to Common Practice Guidelines	Policy Committee, BOH
10/17/20223	Gabbi DeWitt	Revised language on page 5 1. When a comment is removed, BHCPH will post a reason for removing the comment (e.g., "A comment to this post was removed because it promoted discrimination of a protected class. This is a violation of the Black Hawk County Public Health's comment policy.  New language 1. The <a href="#">Electronics Communication SOP</a> outlines the process for removing comments from social media platforms. When a comment is removed, BHCPH will post a reason for removing the comment (e.g., "A comment to this post was removed because it violated BHCPH Common Practice Guidelines.")	Policy Committee, BOH
10/17/2023	Gabbi DeWitt	Revised page 11 <a href="#">Content Removal Tracking Form</a> to reflect fields in Excel tracking document. Link to document added to title.  Added fields: Original Post (link to screen shot), Post ID (if available), What was removed, Username, Link to user social media profile, Link to screenshot of removed content  Revised fields: Social media account from which comment was removed to Social Media Platform  Removed: Attach screen shot of conversation or post or insert image below. Links to screenshots are now part of the form.	Policy Committee, BOH

Micah Knebel	01/2025	No changes right now. May have updates later this year.	Policy Committee BOH
--------------	---------	---	-------------------------