NATIONAL ASSOCIATION OF Community Health Centers

Health Center Operations Resource Packet:

Sample Internal Guidance for Handling Unauthorized Individuals at Health Center Locations

February 4, 2021

Health centers are serving on the community frontline, providing essential COVID-19, primary and preventative health care services. Simultaneously, health centers may be seeing an increased threat from unauthorized individuals entering health center properties to intentionally provoke confrontation with staff. These individuals may represent a variety of alternative interests that intend to disrupt center operations and record and disseminate negative interactions with center staff on social media.

This packet contains operational guidance developed and contributed by health centers that have recently experienced interactions with self-identified "First Amendment Auditors" and/or "Citizen Journalists", attempting to record confrontations with center staff regarding federal funding and "public" access to a health center location.

This guidance is intended to support health center staff in understanding and fulfilling their role in a potential confrontation with an unauthorized individual(s) and subsequent follow-up actions, while upholding the health center mission to serve all members of the community in accordance with Board approved policies and internally issued organizational procedures.

These materials are offered as general samples for health centers to consider as they determine the most appropriate and tailored operations for their organization, staff, patients, and community.

Seek the advice of counsel licensed in your state to determine your specific rights if unauthorized individuals seek to disrupt or protest activities in or near your health center. It is not necessarily the case that such individuals have a constitutional right to be on the premises. Consult with local counsel and law enforcement to understand applicable State and City/Local regulations regarding firearm carrying, intruder de-escalation, safety protocols, trespassing on private property and signage.

Enclosed Samples:

1. "**Guidance on Unauthorized Individuals at Health Center Locations**" – this short procedure template provides basic guidance that can be swiftly drafted and implemented.
2. "**Security Management Plan**" – this short procedure outlines overall security for the organization, with specific sections addressing "unauthorized individuals" and "unauthorized electronic or other recording on health center property".
3. "**Crisis Communications Plan**" – this robust document establishes standards across the health center for coordinating internal and external communications in the event of an emergency crisis.

Special thanks to the health center leaders and expert consultants of the following organizations for their generous review, input and/or sharing of their materials for use by the national network of community health centers:

Family Health Centers (KY), Siouxland Community Health Centers (IA), Iowa Primary Care Association, Primary Care Association Emergency Management Advisory Coalition (EMAC), Feldesman Tucker Leifer Fidell LLP

Additional information and resources can be found at:

Health Center Resource Clearinghouse - "Emergency Preparedness: Tabletop Exercises"- The Centers for Medicare & Medicaid (CMS) requires that health centers test their emergency preparedness plans annually. A tabletop exercise may satisfy this requirement while providing valuable training opportunities for staff. This resource developed by the National Nurse-Led Care Consortium (2019) includes a Terrorism/Active Shooter exercise. The Health Center Resource Clearinghouse contains other Emergency Preparedness and Crisis Communications materials.

Primary Care Association (PCA) Emergency Management Advisory Coalition (EMAC) – This partnership of non-profit organizations serve community health centers and strive to support health centers in being prepared for, respond to, and recover from emergencies that affect the delivery of care.

For inquiries about this document, contact trainings@nachc.org

This project is supported by the Health Resources and Services Administration (HRSA) of the U.S. Department of Health and Human Services (HHS) as part of an award totaling $7,287,500 with 0 percentage financed with non-governmental sources. The contents are those of the author(s) and do not necessarily represent the official views of, nor an endorsement, by HRSA, HHS, or the U.S. Government. For more information, please visit www.HRSA.gov.

Table of Contents

Sample Procedure: Guidance on Unauthorized Individuals at Health Center Locations

Insert Month Year

Procedure: Any person(s) who comes to a Health Center location without an appointment may be considered an "unauthorized individual". [MODIFY/INSERT your Center's definition of "unauthorized"].

At times, an unauthorized individual may try to be disruptive to operations or film/photograph locations without permission from the facility. While there is a low likelihood of disruptive unauthorized individuals coming to our Health Center (HC) locations, the following is guidance and procedures for staff to follow if there are unauthorized individuals at HC locations, including COVID-19 testing locations. These individuals could potentially want to create a scene or disturbance that they can film and post online. Remaining calm and professional will make it difficult to escalate the encounter.

1. Alert the Front Office Manager (FOM) at your site that unauthorized individuals are on-site and causing disruption.
2. If there is security on-site at this time, alert your Security Personnel to assist.

SITE	DESIGNATED PERSON	BACKUP DESIGNATED PERSON
Health Center Location #1	Insert Name	Insert Name or "TBD"
Health Center Location #2		
Health Center Location #3		

3. Front office manager (and Security) or another designated person will:
    a. Ask the individual(s) if they are a patient or if they have an appointment for services (or other appointment with staff).
        i. If "yes" ask the individual(s) for details to confirm. Let the individual know they may not film other patients or staff. If the persons refuses to stop filming, respectfully ask them to leave the premises.
        ii. If the individual says "no", let them know that they may not film patients or staff members, and respectfully advise them that you have been instructed to ask them to leave the premises.
    b. If individuals refuse, become argumentative or threatening in any way, step away and contact the police immediately with complaint about a "trespassing individual". [INSERT your Center's definition of "trespassing"]. Do not engage with them further.
    c. Inform waiting patients they should remain in their cars or wait inside the facility until the confrontational individuals are removed from the property.

4. Front office manager (and Security) or other designated persons will notify Chief Operations Officer of the incident ext. xxx as soon as it can safely be done.

5. Site leadership to be notified about the situation (INSERT CONTACT DETAILS).

6. Director of Communications [INSERT EMPLOYEE NAME] to temporarily deactivate the HC Facebook site.
    a. Account/Settings & Privacy/Your Facebook Information/Deactivation and Deletion/ Temporary Deactivation.
    b. Can temporarily Remove Contact Us Page from External Website if deemed necessary.
    c. Can temporarily deactivate other social media if necessary.
    d. Universal statement can be provided to media outlets if needed.

7. Incidents will be documented and reviewed internally and at Environment of Care committee meetings.

Plans will be shared and updated with Security and partnering COVID testing organizations, as appropriate.

Sample Procedure: Security Management Plan

Policy#	xxxx-xxx	Manual	Security Policy
Department	Security	First Approval Date	month/date/year
Scope	Entire Clinic	Revision Date(s)	
Related Form Procedure/Process		Current Approval Date	
Next Review Date	2021	Date(s) Announced to Staff	

Purpose	To provide a safe and secure environment to protect staff, patients, and visitors from harm.
Mandated by	AAAHC; HRSA
Definitions	• N/A
References	• N/A

1. The Facilities Manager oversees the processes developed to ensure, implement, and maintain the security of the organization.

2. All employees are responsible for the security of the building and responsible for the security of his or her access badge. All [INSERT NAME of your Community Health Center] employees, during working hours, will wear an access badge (name badge).
    a. All employees are to keep his or her access badge in plain sight and above the waist.
    b. Employees are not to deface the front of the access badge (i.e., stickers over pictures).
    c. If there is significant change to the employee's appearance from the photo or the access badge is no longer legible (i.e., worn name/picture), employees are to request new badge through Human Resources.
    d. When an employee misplaces an access (name) badge or if an employee is no longer employed, the Human Resources (HR) Director or designee deactivates the access badge immediately (see Security Access Termination Procedure #xxxx-xxx).
    e. Employees are not to allow other individuals access into the building at any time with his or her access badge.
    f. Employees are not to allow others to allow other employees, visitors, patients, or family members to use his or her access badge at any time.

3. Entrances and doors are secure:
    a. All outside doors, except for the patient entrance, are always locked.
    b. After business hours, the front door is locked.
    c. The last employee exiting the building will page overhead to ensure that no other employees are present in the building and set the security alarm after he or she has determined that building is vacated.
    d. Employees are not to share door codes with anyone, including family members, vendors, patients, former employees, or friends.
    e. Employee family members may utilize exterior entrances only when accompanied by the employee. If the employee is not available, the family member must enter through the patient entrance.

4. Security staff is present throughout the day and beyond company operational hours.
   Security staff:
    a. Confirm all doors are secured throughout the building.
    b. Monitor property through designated walk throughs of the building and property and the use of video surveillance. Depending on the camera in use, the memory is saved for approximately 14-30 days [INSERT recording lifespan based on Center's specific security system, 14 days is recommended minimum]. If the information requires storage beyond that time, Security staff save it to a disk, and file it with any other pertinent information.

5. Vendors:
    a. All vendors are requested to use the receiving entrance unless otherwise pre-arranged.
    b. The vendor sounds the door buzzer and the Operators/designee allow the vendor to enter.
    c. Designated employees are paged to go to the receiving door to sign for packages.
    d. All contractual vendors accessing the building will do so during routine business hours. The vendor is issued a temporary access badge by the maintenance staff at Community Health Center (CHC) and the Site Manager and the badge will be returned at the close of business each day.
    e. Pharmaceutical vendors utilize the patient entrance and are appropriately directed by the Medical Customer Service Representative.
    f. At [INSERT CHC or SPECIFIC SITE LOCATION], deliveries are to be made to the employee entrance and use the buzzer system or per the front entrance.

6. Unauthorized individual(s):
    a. Signs are posted on the CHC property regarding unauthorized individual(s) not allowed (see sample signage below).
    b. Unauthorized individual(s) is/are informed of the need to vacate the property per CHC security team or a member of leadership.
    c. If the individual(s) demonstrate non-compliance (failure to leave), the CHC security staff/ leader/provider are to notify the Facilities Manager or CHC Site Director similarly inform the individual(s) of the need to vacate the property.
    d. The Police Department is notified if the individual(s) remains on the property and refuses to leave. Request the Police Department to assist.

7. Unauthorized electronic or other recording on CHC property:
    a. Signs are posted on the CHC property stating unauthorized recordings are not permitted without written authorization from the Health Center Chief Operating Officer [INSERT authorizing position here].
    b. Individual(s) is/are informed to discontinue recording by the CHC security team or a member of leadership/provider in the CHC.
    c. The Police Department is notified of a "trespassing individual" if the individual(s) remains on the property and refuse to discontinue recording.
    d. If the individual(s) fails to comply, the security staff/leader/provider are to notify the Facilities Manager or CHC Site Director who will similarly inform the individual(s) of the need to discontinue recording.

8. General Safety
    a. No employee is to discuss building security concerns, policies, or procedures in front of patients or with any visitor or non-employee of CHC.
    b. The building and the grounds will have adequate exterior and interior lighting that illuminates all entrances and parking areas.
    c. Patient and employee parking are arranged to assure immediate access by fire or other emergency vehicle to the building.
    d. Emergency buttons are in Pharmacy, Medical, and Dental front desk and used to access the police automatically if the need arises. [INSERT your Center's emergency notification system, e.g., intercom codes, paper/hand signals, EHR alert].
    e. Patients and Visitors
        i. All patients and/or visitors are required to check in with the Medical/Dental Customer Service Representative or be escorted during his or her stay.
        ii. An employee member must accompany all patients and visitors beyond the lobby.
        iii. All employees are to notify Security of any anticipated visitors prior to the scheduled arrival time. This information includes employee to be visited, scheduled time of arrival, door of entry, and approximate length of visit.

9. For any incidents involving the security of patients, visitors, employees, or property, employees are to call the Security team for the investigation.
    a. These incidents are reported utilizing the event reporting process.
    b. The Security Supervisor reviews the documentation and forwards to the Facilities Manager and the Chief Executive Officer (CEO).
    c. The event is reviewed by the Safety Committee who will determine if any further action needs to be taken.

10. [INSERT your Center name here] have security procedures in place for the following actions:
    a. In the event of a security failure: Security will be notified immediately of any situation. Security will address the issue and report any problems to the Facilities Manager and/or CEO for assistance at the CHC.
    b. In the event of civil disturbances within the surrounding areas, the CHC will close and patients/visitors/employees escorted to safety by local police with the possibility of Security protecting the property.

c. Media events:
    i. If an adverse media event occurs involving CHC, the emergency communication plan is implemented (see below).
    ii. Ensure the Center's designated Public Information Officer (PIO) is guiding staff as appropriate.
    iii. Specific visitors (government officials/candidates, surveyors, guests) may require additional security interventions to secure the environment. Outside assistance may be used to assist, at the direction of members of the marketing team.

11. Security policies and procedures are enforced by departmental managers.

12. During initial orientation, all new employees review the Security Management Plan and related policies and procedures. Following the orientation process, all new employees are required to be familiar with minimizing security risks for personnel, emergency procedures to be followed during security incidents, and processes for reporting security incidents involving patients, visitors, employees, and property.

13. Ongoing in-service education are done at a minimum of annually or when plans, processes and procedures are updated, as required by CMS Emergency Preparedness rules.

14. The Safety Committee reviews the Security Management Plan for its objectives, scope and performance on an annual basis and report to the CEO.

PHOTO – signage referenced in Section 6 and 7 of the Emergency Management Plan

Sample: Crisis Communication Plan

[INSERT Community Health Center NAME]
Crisis Communication Plan (Date)

Table of Contents **Page**

Crisis Defined

A crisis or emergency is defined as any situation which:

- Requires immediate and coordinated action.
- Presents threat of significant impact on the operation or reputation of the health center.

Purpose

The purpose of the crisis communication plan is to establish standards in coordinating internal and external communications in the event of a crisis or emergency. While each situation will require a unique public information response, the plan is designed to guide best practices for managing communications with employees, internal stakeholders (patients, board members, contracted providers and/or services), external stakeholders (local/regional officials, vendors/services, affiliate organizations, community-based partners), and the public (news media, legislative offices, state public health officials, national associations).

Objectives

Objectives of this plan are as follows:

- Identify crisis communications team responsible for coordinating public information response in a crisis or emergency.
- Define roles of the crisis communication team and coordination with other internal teams that may be activated in a crisis or emergency.
- Equip communications team with standard procedures and best practices to uphold the mission and values of [INSERT Community Health Center] with both internal and external stakeholders.
- Manage messaging and distribution of messages to employees, the public, and media.
- Create a unified message that can be shared with all internal staff so that each employee understands their role in the crisis and can take appropriate action. Share, repeat and update often.

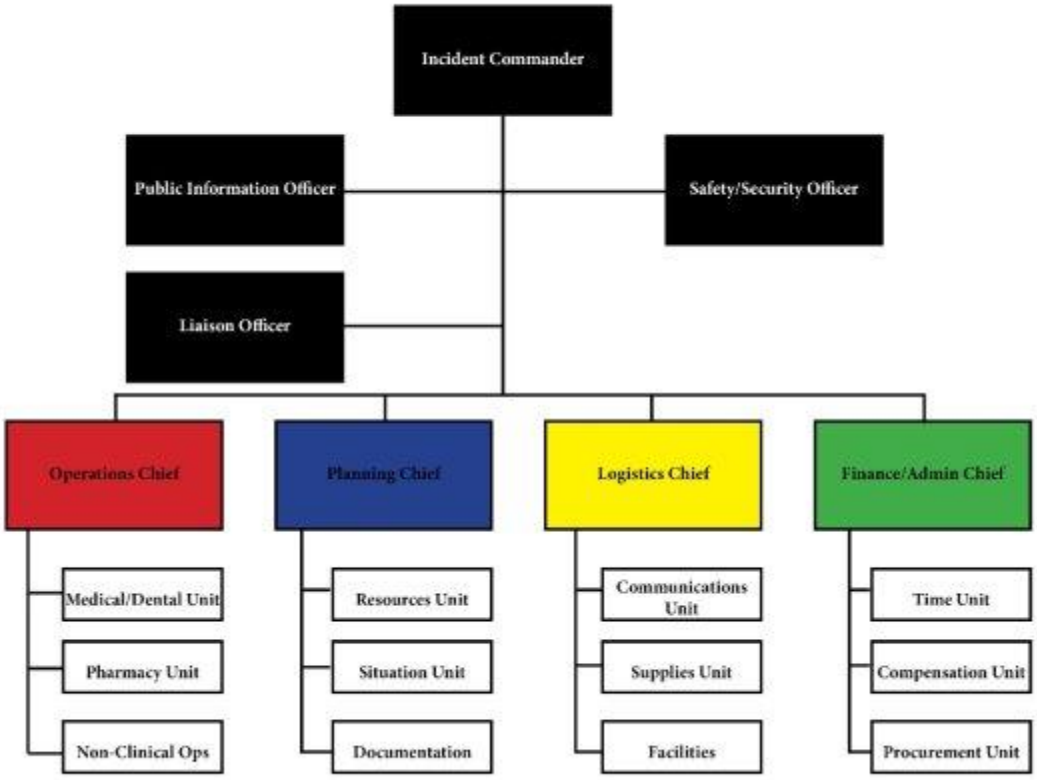
Organizational Threats

The following table provides examples of incident types that may prompt activation of the crisis communication plan.

Type of Incident	Definition	Examples
Human Safety	A human-caused threat to the health center, or the safety of employees, patients, visitors, and vendors	• Sabotage • Current or former employee threat • Patient disruption • Intruders, civil unrest/disruption • Violence/Active Shooter
Environmental Natural Disaster Community Impact	A naturally occurring event that poses risk to the facility including significant damage to the building or threatens the health and safety of employees, patients, and visitors	• Biological/disease • Power/ utility (water, sewer, electrical, gas, steam, HVAC) outage • Tornadoes/Severe weather/Flooding
Financial Management	An internal event that threatens financial stability or disrupts organizational management	• Robbery/theft/fraud • Cyber attack • Inaccurate financial reporting • Leadership misconduct • Threat of lawsuit • Upper management transition / scandal/ succession
Political Legislative Media Issues	A threat to the health center that poses risk to financial stability, disrupts operations, or damages organizational reputation.	• Federal funding • Political protest/ instability • Unfavorable media coverage • Slander/social media feedback related to political action

Crisis Management

As part of the organization's Emergency Management Plan, [INSERT CHC] has adopted the Incident Command Structure (ICS) to manage and coordinate clinic activities during an emergency. The ICS is designed to facilitate decision-making and is flexible for small and large-scale events that may threaten business continuity. The ICS organizational chart is depicted below to illustrate each functional area. Currently, each position is assigned to a designated staff person and alternate and is reviewed and updated annually concurrently with the SCHC Emergency Management Plan. The current ICS chart and descriptions for each position may be referenced in Appendix 1.



When an event occurs that does not prompt activation of the ICS, the directors' team will coordinate crisis management as applicable to the administrative, financial, and clinical operations of the health center. The directors' team is comprised of the following positions:

- Chief Executive Officer (CEO)
- Chief Financial Officer (CFO)
- Chief Medical Officer (CMO)
- Director of Clinic Operations
- Human Resources Director
- Director of Fund Development and Advocacy
- Director of Strategic Planning
- Medical Director/Quality Director
- Dental Director

Additional staff members may be called upon to assist with crisis management. This may include, but is not limited to the Facilities Manager, Security Supervisor, Marketing Coordinator, Emergency Management Lead.

Crisis Communication Team

The crisis communication team is responsible for disseminating information to internal and external stakeholders during a crisis, including the media. The Public Information Officer (PIO) is responsible for assigning tasks among team members as the crisis develops. The PIO will work jointly with the CEO to develop messaging. When the crisis impacts a specific functional area, the director responsible for that department or service will assist with developing messages. Other members of the crisis communication team will fulfill the following roles as assigned:

Task	**Task Roles:**
Situation Assessment	• What is happening internally and externally in response to the crisis? See Appendix 2 for Situation Assessment Checklist
Internal Communications	• Communicate information regarding crisis to board of directors, leadership team, employees, and legal counsel when applicable. • Coordinate messaging through channels including [INSERT YOUR Instant Messaging (IM) Platform] email, and manager briefings. • If the crisis occurs outside of operational hours and disseminating information is critical or time sensitive, IM or a phone tree will be used.
Traditional Media	• Prepare and distribute media releases. • Designate a contact person for media inquiries. • Participate in or appoint designee as necessary to participate in media interviews.
Social Media	• Monitor social media platforms (Facebook, Twitter, etc.) for posts regarding the crisis. • Ensure posts or comments in response to the crisis are consistent and coordinated with other messaging.
External Communications/ Record Keeping/ Messenger	• Document critical conversations, decisions, details, and media questions regarding the crisis to effectively evaluate crisis communications management. • Relay messages and other important communications to other members of the crisis communications team.

Developing Key Messages

The crisis communications team will develop factual, responsive messages for internal and external messages. It will also provide a script for operators and the voicemail system. All media and public inquiries should be referred to the Public Information Officer.

- Messages should be prepared for media inquiries, member updates, and proactive phone calls to critical audiences.
- Messages should reflect the organization's overall messages, leadership role, and resource status. They should attempt to reinforce the positive and be action/solution oriented if possible.
- Consider what media know about the situation and what their potential interest is.
- Recognize that unfavorable, inaccurate information, if not corrected, could have future negative consequences requiring additional responses.
- Consider questions that will be asked to prepare answers for them – including the questions you hope will not be asked.
- Develop a written statement for phone operators and the representative greeting members of the media and the public. Decide if it is appropriate to change the organization's or particular staff members' voicemail messages.
- Consider need for additional materials such as a fact sheet, backgrounder, web site resources, FAQs, etc.
- If applicable, consult with other organizations involved to ensure consistent messages and conformity of responses.
- Take into account linguistic and cultural needs when crafting messages and considering media outlets.

Messaging Best Practices

The following are general guidelines for effectively using traditional and social media to communicate in the event of a crisis. Only the designated spokesperson should release information to the media. All other employees should refer the media to the designated spokesperson if they are approached.

Traditional Media

Traditional media has the ability to frame a crisis, and stakeholders generally adopt that frame. Therefore, it is vital to be aware of the information communicated through traditional media and utilize these sources if necessary.

Digital & Social Media

If a crisis occurs, it is important to respond quickly, accurately, and directly so that our digital media accounts are seen as a credible source of information that stakeholders can count on. Generate short, concise posts for all social media outlets. The posts should contain a short statement about the status of the crisis and provide a link to more information if necessary. Keep all social media outlets consistent with each other and update them as needed.

Always

- Empathize with those affected.
- Be transparent and honest.
- Provide timely, or "just in time" updates as information is confirmed. Too few, too little, too late are common pitfalls.
- Seek information from experts in the field.
- Ensure channels for two-way communication.

Never

- Say "no comment" (instead say "let us get back to you on that" and follow through).
- Falsify information.
- Promise too much.
- Ignore requests from individuals or the media.

Crisis Communications Timeline and Checklist

Phase I: Immediately Following Crisis Event:

1. Assemble crisis communication team.
2. Assess situation and level of impact.
3. Determine need to activate ICS.
4. Brief leadership team on situation.
5. Inform all staff members of situation using appropriate communication methods (IM, Email, Text, or Phone Tree).
6. Develop key messaging.
7. Inform operators where to direct media calls.
8. Begin monitoring social media.

Phase II: One to 24 Hours Following Crisis Event:

1. Gather known facts and verify scope of event.
2. Determine need to contact outside agencies, resources, or legal personnel.
3. Provide updates to employees.
4. Release initial statements to traditional media and on social media platforms.
5. Designate media staging area, if applicable.
6. Schedule briefings and situation report with crisis communication team.
7. Update messaging as new details are available.
8. Document all communication activities in response to crisis.

Repeat these steps throughout the duration of the event.

Phase III: Post-Crisis Management

1. Debriefing with employees, including resources available for post-crisis recovery.
2. Release follow-up statements to media and social media:
    a. Recap crisis.
    b. Apologize when appropriate.
    c. Explain crisis is not a normal occurrence.
    d. Explain what is being done to repair the crisis, which may mean finding the most current information outside your organization and with the local authorities or lead government agency, like local Municipality, Local or State Department of Health.
    e. Explain what is being done to prevent crisis from reoccurring, if applicable.
3. Directors and crisis communication team debrief:
    a. What worked well?
    b. What challenges were encountered?
    c. What follow-up actions need to be completed to recover from the crisis?
    d. Are there policies or procedures that should be reviewed and modified?
    e. What are the risks of event reoccurring?

Appendix 1: Incident Command Structure (ICS) Organizational Chart and Job Descriptions

[INSERT your Organizational Chart displaying the CHC ICS/Emergency Management Chain of Command naming the Designated Point of Contact and an Alternate].

See examples of recommended roles below:

Incident Commander (usually the CEO) → Public Information Officer; Safety Officer; Liaison Officer; Security Officer
Operations Section Chief; Planning Section Chief; Logistics Section Chief; Finance/Admin Section Chief

Operations Section Chief → Medical Nurse Manager; Dental Nurse Manager; Pharmacy; Non-Clinical

Planning Section Chief → Resources, Situation, Documentation

Logistics Section Chief → Communications; Supplies; Facilities

Finance/Admin Section Chief → Time Unit; Compensation; Procurement

INCIDENT COMMANDER

Line of Authority

The Incident Commander, if not the Chief Executive Officer, reports to the Chief Executive Officer. Per the ICS, the five EOC Section Chiefs report directly to the Incident Commander—including sometimes through the EOC Incident Commander. Per ICS protocols, the EOC provides additional recovery management functions through the Liaison, the PIO, the Safety Officer, and Security. [INSERT/TAILOR based on your Center's Incident Command Structure].

Duties

The Incident Commander is responsible for: activating the clinic EMP, activating and deactivating the EOC, disseminating information to the EOC Incident Commander, management staff and Section Chiefs, directing specific actions as required, approving issuance of press releases, and providing liaison with other agencies. A summary list of overall responsibilities follows.

The Incident Commander will appoint the CHC Chief Medical Officer to develop the medical plan; coordinate the provision of Critical Incident Stress management for staff; and designate qualified personnel to provide medical attention to ill or injured personnel until professional medical help can arrive.

PUBLIC INFORMATION OFFICER (PIO)

Line of Authority

The Public Information Officer is a staff assistant to the Incident Commander and is not in the direct line of authority.

Duties

The Public Information Officer (PIO) advises the Incident Commander on the potential effects of proposed actions on external and internal relations. The PIO serves as the dissemination point for all news releases from the clinic. Other clinic groups that want to release information to the public, employees, stakeholders, or regulators should coordinate through the PIO. The PIO reviews and coordinates all information releases from other clinic sources. The PIO coordinates to ensure that: employees, their families, regulators, and other stakeholders receive timely and accurate information about the clinic's situation. The PIO should follow the communications guidelines already established for the clinic for emergencies. The PIO also prepares fact sheets about the clinic with sidebars about the clinic's business continuity program before interruptions occur.

LIAISON OFFICER

Line of Authority

The Liaison Officer is a staff assistant to the Chief Executive Officer and is not in the direct line of authority.

Duties

The Liaison Officer provides direct support to the Chief Executive Officer. The Liaison Officer is responsible for: answering telephone calls and managing messages from other organizations in government and the private sector; coordinating with key stakeholders in government, including regulators and those with direct service agreements with clinic; requesting assistance directly to other

organizations when there is no formal emergency declaration; and keeping the Chief Executive Officer and Incident Commander informed about concerns and pressures from outside organizations.

SAFETY/SECURITY OFFICERS

Line of Authority

The Safety/Security Officers are staff assistants to the Incident Commander and is not in the direct line of authority. When clinic site security is supplanted or enhanced by outside security (CHP, local law enforcement, FBI), then the line of authority will be a point of coordination between clinic security and external agency security.

Duties

The Safety/Security Officers provides direct support to the Incident Commander. The Safety/Security Officers are responsible for: continuously monitoring the work environment to ensure the health and safety of the clinic personnel and visitors; developing safety strategies for the recovery along with the Incident Commander and the Logistics Section Chief; controlling ingress and egress into the area, including the maintenance of a sign-in and out log; controlling the location of parking and general traffic around the clinic HQ site after a major emergency; verifying identification and reason to enter the EOC or recovery area; preventing criminal acts upon clinic staff or facilities; providing protection for the Chief Executive Officer, PIO and Incident Commander during public press briefings or general public briefings regarding recovery operations. Safety/Security is also responsible for preparing a security plan is coordination with the Logistics Section Chief.

OPERATIONS SECTION CHIEF

Line of Authority

The Operations Section Chief is in direct line of authority, reporting directly to the Emergency Operations Center (EOC) Incident Commander.

Duties

The Operations Section Chief oversees continuity of Operations, assesses response and recovery support situations, and oversees operational response and restoration throughout the clinic's facilities, coordinating with the other Section Chiefs.

PLANNING AND INTELLIGENCE SECTION CHIEF

Line of Authority

The Planning and Intelligence Section Chief is in direct line of authority and reports directly to the Incident Manager.

Duties

Responsibilities include collecting, analyzing, and displaying situation information; preparing periodic situation status reports with the Incident Commander, and the other Section Chiefs; and developing goals and objectives for the forthcoming operational period's Action Plan (please see the Action Planning and Intelligence forms attached to this plan and document the Action Plan on the Action Planning and Intelligence forms). During each operational period, begin advance planning for forthcoming periods. As the workload decreases, begin planning for deactivation and demobilization. Provide information management and related support to the other Section Chiefs and staff support

positions in the EOC. Keep the Incident Commander updated on significant Planning and Intelligence findings (e.g., advance planning reports, serious changes in weather or safety issues, and projected reductions in resources or support, etc.).

LOGISTICS SECTION CHIEF

Line of Authority

The Logistics Section Chief is in direct line of authority and reports directly to the Incident Commander.

Duties

Responsibilities include transportation, coordination with security, and logistics resources to match the other Section Chiefs' needs.

FINANCE AND ADMINISTRATION SECTION CHIEF

Line of Authority

The Finance and Administration and Administration Section Chief is in direct line of authority and reports directly to the Emergency Operations Center (EOC) Director.

Duties

The Finance and Administration and Administration Section Chief should: monitor incoming information and Action Planning and Intelligence in the Emergency Operations Center (EOC) in order to identify and assess potential impacts on the clinic's financial status, including but not limited to cash flow, extraordinary expenses, budget impacts, and needs for funding to meet the emergency's requirements. The Chief advises the Incident Commander about these impacts and recommends actions to mitigate them. The Chief assists the other Section Chiefs in developing means to identify potential impacts and ways to reduce them. The Chief works closely with the Logistics Section Chief to ensure that expenses related to the emergency are captured and recorded in the formats desired for governmental and insurance reimbursements. The Chief maintains contact with salvage and clean-up contractors to ensure they work effectively to minimize the clinic's costs. The Finance and Administration and Administration Section Chief should also participate in Action Planning and Intelligence sessions and ensure the Finance and Administration and Administration Section Chief is supporting other elements consistent with priorities established in the Action Plans.

Appendix 2: Situational Assessment Checklist

The crisis communications team will assess the situation, determine facts, and begin delegation. Questions to help devise appropriate crisis communications response, include, but are not limited to:

1. Who is the crisis communications lead person responsible for ensuring all steps are taken? (Most likely the designated Public Information Officer).
2. What is the situation? What will happen next?
3. Who are the internal stakeholder/who on staff needs to be involved?
4. What immediate steps need to be taken?
5. What is known and who already knows it?
6. Who are your external stakeholders (e.g. affiliate organizations, community-based partners, local/regional coalitions, or agencies) Is there potential public interest? Does the issue have traction (will it become anything more than a blip on the evening news)?
7. Who will be affected?
8. What are people feeling – what emotions need to be considered?
9. What information is needed and who beyond organizational staff need to get it? When will it be available?
10. What should the organization do about it? Proactive vs. reactive? Contact or refer to another organization?
11. What CAN and CAN'T be said? What are the organization's privacy policies?
12. Is legal or PR counsel needed? This is recommended.
13. Who will communicate response as spokesperson? (Most likely the CEO).
14. How will response be communicated? (Could include: newsletter article – low urgency – also good as a follow up to any major situation; one-on-one meetings – higher urgency, specific audience targeted such as legislators; media release – higher urgency, broad public appeal; media conference – high urgency and big issue; etc.).
15. Should a resource list be compiled of additional spokespeople?
16. What media will be contacted? What legislators? What donors? Other stakeholders? (Consider reaching to your state Primary Care Association for support or assistance).
17. Who will coordinate IM and email notifications and begin the staff and board phone trees?

Appendix 3: Crisis Meeting Agenda

During an initial briefing about the crisis, the following specific agenda items will be reviewed:

1. Situation report: Resource: Incident Action Plan (IAP) Quick Start Template
https://www.calhospitalprepare.org/sites/main/files/file-attachments/hics-incident_action_plan_iap_quick_start_3.docx

   What appears to have happened.
   Confirmed facts (when, immediate known consequences, likely consequences).
   Scope of proposed situation.

2. Initial response status:
   What is being done, why, by whom.
   Likely implementation time and hoped-for results.

3. Initial communications status:
   Who knows, who needs to know immediately and later on.
   Alert switchboard.

4. Short-term response requirements:
   Delegate crisis communications responsibility.
   What must be done in the next several hours and how.
   What human and material resources are available or needed.

5. Short-term communication process:
   Board members, staff, and patients.

6. Next meeting time.

Appendix 4: Tips for Dealing with the Media

Dos and Don'ts of Dealing with the Media during a Crisis

During an emergency **DO**:

1. Release only verified information.
2. Escort the news media everywhere on the emergency site.
3. Have a designated spokesperson.
4. Keep accurate records and logs of all inquiries and news coverage.
5. Learn media deadlines and try to meet them.
6. Provide equal opportunities and facilities for print and electronic media.
7. Have a clear idea of what can and cannot be released.
8. Carefully coordinate planning and implementation of public relations activities with other aspects of the comprehensive emergency plan.

During an emergency **DO NOT**:

1. DO NOT Idly speculate on the causes of the emergency.
2. DO NOT Speculate on the resumption of normal operations.
3. DO NOT Speculate on the outside effects of the emergency.
4. DO NOT Speculate on the dollar value of losses.
5. DO NOT Interfere with the legitimate duties of news people.
6. DO NOT Permit any unauthorized spokesperson to comment to the media.
7. DO NOT Attempt to cover up, or purposely mislead the news media.
8. DO NOT Place blame for the emergency.

General Guidelines for Dealing with the Media during a Crisis

- The Public Information Officer (PIO) or designee will respond in the most expedient manner possible with information for media during a crisis. If the health center does not release information for media, it will come from another source.
- If media initiates contact prior to a crisis decision being made, the PIO or designee will neither confirm nor deny the incident/issue; but will investigate and return the call.
- The PIO or designee will always attempt to coordinate release of information with responding emergency agencies—so both parties release the same information.
- The designated spokesperson should always be thoroughly briefed and constantly updated on status of the incident.
- If the incident appears to be of short duration, an approved follow-up statement will be issued, including a summary of the incident.
- If it appears to be a major, prolonged incident, PIO or designee will arrange for regularly scheduled media update briefings. At each briefing, there will be a recap of the incident and any new information provided.
- If there is important new information, it will be shared with the media as quickly as possible by phone, email, fax and/or special media briefing.
- If possible, coordinate with television/radio stations to come up with a mutually acceptable plan for interviews that will allow live coverage to be carried without giving preferential treatment.
- Clearly state at the beginning of initial briefing that all verified information that the crisis team has will be passed on and there will be no information given off the record. All information will be provided at the press gathering.
- The health center will prohibit release of an individual's name who has been involved in an injury or fatality until his/her family has been notified.
- The health center will not give the media access to the families of anyone injured or killed unless the families expressly grant permission.
- The health center will work in contact with hospital spokesperson(s) when releasing any information regarding an injured person's current condition.
- Document all inquiries and contacts with media in a media log sheet.
- Refer to (INSERT: Disaster Contact List in your Community Health Center Emergency Management Plan for key agency and media contacts].

Appendix 5: Crisis Communication Team Assignment List

Date of Event:	
Description of Event:	
Public Information Officer (PIO):	
Situation Report:	
Internal Communications:	
Written Media Releases:	
Official Spokesperson(s):	
Social Media Manager:	
Record Keeping and Messenger:	