MAJOR PRIVACY BREACH EMERGENCY QUICK REFERENCE RESPONSE GUIDE

ANTICIPATED IMPACT

Moderate to significant when breach involves a large number of individual's protected health information (PHI) or high profile individuals.

1. May disrupt usual operations when computer systems are affected.
2. Taxing to staff and usual operations when significant additional staff time is needed to address the privacy issue or when computer systems are disrupted.
3. Potential stress to those affected by the breach which may be unnecessarily magnified if communication is inadequate.
4. Risk for significant fines and other penalties to facilities and staff for failure to protect health information.

MISSION

To provide a prompt organized response to a privacy breach including mitigation of negative effects.

GOAL	ACTIONS
Coordinate activities with other hospitals, DPH and the community	□ **Report:** Contact the facility Privacy Officer or the general Privacy Office for suspected breaches. □ **Notify** the facility Administrator On Duty (AOD) via the Privacy Officer, or directly during off hours, if the suspected breach is significant or high visibility as follows: ▪ Incidents involving 10 or more affected individuals protected health information (PHI) exposed outside of the facility ▪ Incidents involving celebrities or "VIPs" ▪ Incidents involving media coverage or press release ▪ Incident involving criminal activity ▪ Any other incidents involving reputational, regulatory, and/ or financial risk to SFDPH □ **Help Desk** is notified if IT action is needed. Specify the level of urgency and alert the Information Security Officer. (For Information System failure/ Cyber Attack see reference at the end of this guide.) □ **Convene** an Incident Command / Hospital Incident Command (HICS) response team scaled to the level of response needed. Incident Command would likely include the facility ▪ Administrator On Duty (AOD) ▪ Privacy Officer(s) ▪ DPH and facility Public Relations Officers ▪ Legal representative ▪ Medical Records Director/ designee ▪ Information Security Officer ▪ Regulatory Affairs/ Quality Management Director/ designee □ **Determine if the disruption is deliberate and targeted** by consulting with Incident Commander and senior IT/IS staff; contact SFSD and SFPD, the FBI Cyber-Terrorism Division, and California State Cyber-Terrorism Division or District Office, as appropriate. □ **Initiate call backs** as directed by Incident Command for above persons /others relevant to the case. □ **DPH-Wide Activation:** Incident Command determines if it is appropriate to contact the Department of Emergency Management to report issues and coordinate resource requests. DEM coordinates with the Emergency Operations Center (EOC) for a city-wide response. State and Federal agencies are contacted as determined by local DEM and EOC authorities. ▪ CAHAN (California Health Alert Network) may be used for notifications to multiple facility or DPH-wide staff if a low, medium, or high level alert is warranted.
Take immediate steps to gather	□ **Follow all instructions** from the command post and IT Help Desk. □ **Document** the issue, mitigation steps, and breach decision tree on the privacy breach reporting form

GOAL	ACTIONS
information and mitigate the breach	via the Privacy Officer in collaboration with the Manager of the affected department(s). (Form available at http://www.sfdph.org/dph/files/HIPAAdocs/PrivacyPolicies/RptBreachesPol03112009.pdf) ☐ **Mitigate:** Incident Command (Privacy Officer/s, AOD, Public Relations, Legal representative, Medical Records and IT representatives with others as needed) direct steps to mitigate negative effects. Mitigation may include but is not limited to: ▪ Disabling access to affected computer systems ▪ Organizing a search to retrieve lost data ▪ Securing areas or systems to prevent additional breaches ▪ Law enforcement activities ▪ Communicating to stakeholders
Communicate to further mitigate and direct response	☐ **Incident Command** determines level of response and initiates activities as needed, such as staff call back, searches, IT Help Desk support, etc. ☐ **Mitigating Misinformation:** Direct staff to refer questions to Incident Command and refer media to the Public Relations designee. ☐ **Public Relations** crafts messages w/ Incident Commander approval to staff / community/ media ☐ **IT works w/ Public Relations to** Post approved messages / FAQs on DPH site as needed to communicate to community. ☐ **Privacy Officer(s)** Document to track incident and response activities and use information for Incident Command decision-making, to determine information and directives to be disseminated, and for required reporting. (Use of HICS 252 to track activities preferred. ☐ **Regulatory Affairs/ QM Director** or designee collaborates with Privacy Officer(s) to prepare letters to notify affected individuals and regulatory bodies (below) using available templates
Report to Regulatory Bodies	☐ **Report** to regulatory bodies as required (by Privacy Officer or Legal Dept. Rep): ☐ **Immediately** report breaches of 500 or more to the Department of Health and Human Services Office for Civil Rights at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html ▪ Breaches of less than 500 must be reported to above no later than 60 days after the end of the calendar year in which the breach occurred ☐ **Hospitals** are required to report *suspected* privacy breaches within 15 calendar days of awareness of issue to the California Department of Public Health (CDPH) by telephone and in writing ☐ **Community and Behavioral Health Services** (CBHS) are required to report to DHCS immediately by phone and in writing within 24 hours with a written conclusion and plan of correction within 10 days.
Restore normal operations as soon as possible.	☐ Notify staff and debrief. ☐ Public Relations to post messages on DPH site to communicate a summary of events and closure. ☐ Continue to follow up with training and other post-incident steps

OTHER REFERENCES

DPH Privacy Policies available at http://www.sfdph.org/dph/comupg/oservices/medSvs/HIPAA/HIPAAPolicies.asp

- HIPAA Compliance – Reporting of Unlawful or Unauthorized Access of Protected Health Information at http://www.sfdph.org/dph/files/HIPAAdocs/PrivacyPolicies/RptBreachesPol03112009.pdf (includes link to reporting form)

DPH Data Security Policies available at http://www.sfdph.org/dph/comupg/oservices/medSvs/HIPAA/HIPAADataSecPolicies.asp

DPH Media Policy available at http://www.sfdph.org/dph/files/PoliciesProcedures/EXF2_MediaPolicy.pdf

Facility / Site-specific privacy and emergency response policies including:

SFGH Hazard Specific Plans: Information System Failure / Cyber Attack available at http://10.84.4.135/SFGHDisasterPrep/Hazard%20Specific%20Plans%202013.pdf

LH Hospital Wide Policy 70-02 Emergency Response at http://in-sfghweb01/LHH/policies/Policies.htm