Monterey County Board of Supervisors

Response to the

2014 Monterey County Civil Grand Jury Interim Final Report No. 12

July 28, 2015

TABLE OF CONTENTS

Page(s)

REPORT TITLE: Information Security at Natividad Medical Center: A Model of Best Practices
RESPONSE BY: Monterey County Board of Supervisors
RESPONSE TO: Findings F-1, F-2, F-3, F-4, F-5, and F-6

F1. The separation of Natividad's IT Department from the County's IT Department in 2009 was warranted, due to unique regulations and auditing standards for health provider institutions.

Response to F1:

The Board agrees with this finding. Natividad Medical Center(NMC)'s Information Technology (IT) Department separated from the County's IT Department resulting in NMC assuming full authority and control over the hospital's IT systems. This action was essential given the rapidly advancing medical technologies for the provision of safe, high-quality health care and protection of patient's health information with robust privacy and security practices responsive to unique regulatory and performance requirements for health care institutions.

F2. Natividad Medical Center is exemplary of best practices in its protection of patients PHI.

Response to F2:

The Board agrees with this finding. NMC does strive to adopt best practices where applicable. Best practices by nature perpetually evolve. As such NMC will continue to evaluate and refine processes in an ongoing effort to maximize process improvements.

F3. Natividad Medical Center has 24/7 IT Department staff well-equipped to prevent cyber-attacks.

Response to F3:
The Board agrees with this finding. NMC IT maintains 24x7 IT Coverage to respond to applications, network, system outages as well as security incidents.

F4.Natividad Medical Center minimizes downtime of IT networks by dedicated, continual monitoring.

Response to F4:

The Board agrees with this finding. NMC IT actively monitors applications, hardware and logs for the purpose of sending alerts when critical errors occur that require action. System performance information such as memory, storage, and processor usage is also captured for the purpose of trending and scaling the infrastructure.

F5. Language translation services should be utilized in preparing written notices to persons impacted by PHI breaches whose common language is other than English and Spanish.

<u>Response to F5:</u>

The Board wholly disagrees with this finding. Page six (6) of the Grand Jury's Final Report No. 12 entitled "Information Security at Natividad Medical Center: A Model of Best Practices" acknowledges the readiness of the medical center to communicate in languages of the people it serves, including multiple dialects.

Persons who are impacted by a Protected Health Information (PHI) breach are noticed in a language they understand. The written notice templates are in English and Spanish. However, when the person impacted speaks a language other than Spanish or English the document is translated to the appropriate language. If the person impacted speaks an indigenous language and written translation is not possible the notification is "sight" translated either in person or by phone.

NMC has translated the Breach Notifications templates in the languages used by the two greatest numbers of its patients.

F6. A weak link exists in security of PHI with hand-delivered paper documents.

<u>Response to F6:</u>

The Board agrees with this finding.

REPORT TITLE: Information Security at Natividad Medical Center: A Model of Best Practices
RESPONSE BY: Monterey County Board of Supervisors
RESPONSE TO: Findings F-1, F-2, F-3, F-4, F-5, and F-6

R1. Natividad Medical Center share its IT Department model with other county hospitals as a standard of excellence when appropriate at all upcoming opportunities.

Response to R1:

The Board agrees with this Recommendation. NMC's IT Department regularly collaborates with all hospital IT departments within Monterey County including the recent formation of Central Coast Health Connect, the regional Health Information Exchange (HIE). We will continue to share our IT expertise with our colleagues.

NMC is a member of the California Association of Public Hospitals and Health Systems (CAPH) representing the 21 California public health care systems which are the core of the state's health care safety net. Since 1999, the California Health Care Safety Net Institute (SNI), serving the members of CAPH, has helped public health care systems develop and spread innovative programs to help improve the quality of patient care and care coordination, enhance efficiencies, and eliminate health care disparities. NMC IT leadership has recently joined a new SNI collaboration to standardize IT processes of its members. The group had its kick off meeting in May and will be meeting regularly. We will collaborate and share our knowledge.

R2. Natividad Medical Center immediately review and ensure that its notices to the public about HIPAA breaches are written in languages commonly understood by the impacted person.

Response to R2:

The recommendation has been implemented. On June 26, 2015 NMC reviewed its notices to the public about privacy breaches process to ensure the notice is written in a language commonly understood by the impacted person.

Upon admission each patient is asked their preferred language and this is documented in the medical record. NMC uses this information to draft the privacy breach notification in the appropriate language including or to determine if any sight translation may be required.

In the development of the interpretation program, NMC patient demographics were studied and it was found that there were sixty (60) languages spoken in the service area including indigenous-languages, primarily Triqui, Mixteco, Zapoteco and Chatino all native to Oaxaca, Mexico. The study also found fifty percent (50%) of the patient population spoke English, forty-seven percent (47%) spoke Spanish and three percent (3%) spoke one of at least fifty-eight (58) other languages.

NMC is in full compliance with the California Health and Safety Code §1259 requiring NMC to provide language assistance services for language groups that comprise five percent (5%) or more of the facility population. NMC exceeds the regulation with interpreter services available 24 hours a day to all patients even if less than five percent and if a document requires translation there are

interpreters readily available to either translate the document in written form or to provide sight translation.

R3. Natividad Medical Center continue to improve and update best practices for secure physical delivery of PHI documents to other healthcare providers and individual patients while awaiting an active HIE for secure transmittals.

Response to R3:

The recommendation has been implemented. Investigations of privacy breaches during the calendar year 2015 reveal privacy breaches are related to documents being printed for delivery to the patient. For example, discharge instructions, receipts for payment, and prescriptions that are labeled with incorrect label or an incorrect document is given to a patient or their representative.

Based on these findings NMC has taken the following actions over the past four months to implement best practices and mitigate future breaches:

1. Printing of discharge instructions has been restricted in the Emergency Department to Registered Nurses staff only.
2. The medial staff has been encouraged to use only electronic prescription rather than hand written ones that require a patient label.
3. The nursing staff have been instructed to use two patient identifiers (patient name and date of birth) for care and treatment of patients that include the review of discharge instruction documents.
4. The nursing staff in the Emergency Department has been instructed to check each document as it is removed from the printer to ensure another patient's document did not print in the middle of the print job.
5. The staff who receives payments have been educated to verify the patient name and credit card number (when appropriate) prior to providing a receipt.

NMC will continue to investigate the root cause of each privacy breach and determine the corrective action to prevent future re-occurrence, including research to improve and update best practices for secure physical delivery of PHI documents.