Monterey County Board of Supervisors

Response to the

2013 Monterey County Civil Grand Jury Interim Final Report No. 5

August 26, 2014

TABLE OF CONTENTS

REPORT TITLE: Privacy and Security of County On-Line Data and Information
RESPONSE BY: Monterey County Board of Supervisors
RESPONSE TO: Findings F-1, F-2, F-3, F-4, F-5, F-6, F-7, and F-8

Finding F-1: During the past eight or more years, the Monterey County government has not devoted adequate attention to compliance with the California and Federal Privacy Laws, and must now immediately change this attitude to strict attention and compliance, if it is to avoid serious financial consequences for potential violations.

> ***Response F-1:*** The Board disagrees partially with this finding. The Board notes that Information Security experts currently advise U.S. government organizations, including federal, state and local agencies, that compliance with privacy laws is important and necessary. The Board agrees that compliance with laws regarding the privacy and security of legally protected data and information is important. The Board does not agree that the County has devoted insufficient "attention" to legal compliance and disagrees that an "attitude" exists needing change. The Board observes that it has taken significant measures to ensure such data is protected and will continue to do so in the future.

Finding F-2: The present old and defective Privacy and Data Breach Notification Policies are to be replaced immediately and the newly developed 2014 versions disseminated promptly to all Department heads now that they have been approved by the Board of Supervisors. This must be quickly followed-up by education of all County employees as to these new rules, and the appropriate conduct required when using or operating County IT and communication systems.

> ***Response F-2:*** The Board disagrees partially with this finding. The newly developed and approved 2014 County policies on privacy and data protection have replaced prior versions as of the date of this response. Dissemination of the new policies has been completed and education regarding them and appropriate usage of County information technology resources is continually provided to the county work force. The Board disagrees that the former versions of its privacy and data policies can be characterized as "defective."

Finding F-3: County Counsel's office has not been adequately aware of these Privacy issues in the past, in part because of inadequate staffing and education of its lawyers, but it is now actively trying to change this situation within its budget limitations. However, it clearly needs additional funding to address these issues and to assist the IT Department and other County departments with this complex area of the law.

> ***Response F-3:*** The Board disagrees partially with this finding. It disagrees that County Counsel's office has not been "aware" of privacy issues. The Board observes that County Counsel, like all County Departments, must operate within fiscal constraints. The Board further observes that County Counsel is devoting resources to obtaining additional training and education in the area of data privacy and security. For example, it is planned that a Deputy County Counsel will undergo training by the International Association of Privacy Professionals (IAPP) in the area of data privacy and security, will

obtain certification in the area, and will, in turn, educate other attorneys in the County Counsel's Office on these subjects. Also, attendance is planned at an IAPP Privacy Conference in September 2014.

Finding F-4: The County IT Department needs to continue its active pursuit of software and hardware means of preventing intrusions, and keep the Chief Administrative Officer (CAO) and his staff fully aware of the extent of this problem and the costs involved in complying. This activity may require that the CAO recommend changing some aspects of the Zero-based budgeting methods currently used to allocate funds to the IT Department to pay for necessary personnel and software. This possible change in budgeting methods is something that should not be postponed beyond the current fiscal year.

> ***Response F-4:*** The Board disagrees partially with this finding. It agrees, however, with the bulk of this finding and observes that the activities it describes are presently underway. Funding for upgraded intrusion detection systems and a next generation firewall has already been requested and has been obtained through the capital replacement program. The County Information Technology Department keeps the CAO advised of needs in this area. The Board will consider all available fiscal mechanisms to provide funding for these activities.

Finding F-5: Everyone involved must realize that this area of the law is in a constant state of change, both at the state and federal level, and that there may even be some aspects of international Privacy laws that come into play at times, even for locally stored data.

> ***Response F-5:*** The Board disagrees partially with this finding to the extent that it implies lack of awareness of the fact of continuous change and scope in data and security law. The Board agrees that privacy laws affecting County data should be monitored.

Finding F-6: Of particular concern should be those Privacy laws relating to health records used or maintained by County agencies like Natividad Medical Center and the County Health Department since the provisions of the Federal HIPAA law are particularly burdensome and the penalties very expensive if violated.

> ***Response F-6:*** The Board disagrees partially with this finding to the extent that it implies lack of awareness of laws pertaining to health records and agrees that Federal HIPPA laws are important yet burdensome regulations that must be followed closely. The Board observes that the County has access to and avails itself of expertise on HIPPA and similar laws governing health records.

Finding F-7: County departments and those agencies and personnel involved in acquisition of communications, software and almost every other type of goods and services, must insist both contractually and in practice that all vendors at every level comply with required Privacy and Breach Notice laws when dealing with County owned or controlled personal data and information. Unfortunately, many commercial vendors and businesses are not currently in compliance, worldwide, as can be seen from the numerous data breaches recently reported in the U.S. news media.

Response F-7: The Board disagrees partially with this finding. It agrees with this finding to the extent that it asserts that county vendors should be involved with compliance with security and privacy laws, and should cooperate in safeguarding county data and information. The Board observes that the County continually makes efforts to procure legal compliance and cooperation from vendors. The Board is not able to make conclusions about whether "many" vendors and businesses comply with applicable laws.

Finding F-8: Finally, Monterey County is not unique in dealing with these critical Privacy problems, according to a story in the IAPP newsletter in late May 2014. This publication reported that the Los Angeles (LA) County Board of Supervisors recently voted to direct its county staff to promptly develop a plan to require third-party contractors hired by the County to "encrypt sensitive information on their computers as a condition of their contracts." This followed the February 2014 breach of data on eight computers holding 342,000 patients' medical records taken from the offices of contractor Sutherland Healthcare Solutions. LA County already mandates that county laptops be encrypted. These new rules now also require that all county department's computer workstations' hard drives are to be encrypted.

Response F-8: The Board disagrees with this finding. It is not able to agree or disagree with the accuracy of news stories reported by IAPP or other organizations, nor is it able to comment on policies which may or may not have been adopted by other counties. The Board observes that County Security Policy, section, 1.16.3.1.4.7, states that protected information transferred to laptops, PDA's and all other portable media shall be encrypted.

REPORT TITLE: Privacy and Security of County On-Line Data and Information
RESPONSE BY: Monterey County Board of Supervisors
RESPONSE TO: Recommendations R-1, R-2, R-3, R-4, R-5, and R-6

Recommendation R-1: The Monterey County Board of Supervisors and their staff should carefully study this Report on Privacy problems, in conjunction with its CAO, the County Counsel and his Privacy Deputy, and the Director of County Information Technology and her Security Chief and other IT personnel. These are key people since they directly work in the field of privacy, prevention of data breaches, and in coordinating the design and operation of the County website. The study of these issues has a dual purpose of understanding the significant penalties and financial risks to the County government due to the complexity of the laws, *and* realizing that there are some expensive and complex technical issues in this aspect of County business operations.

> ***Response R-1:*** This recommendation has been implemented, although there is no current post of "Privacy Deputy" in the County Counsel's Office. Appropriate personnel have reviewed the grand jury's report on privacy carefully and will do so again in the future, as circumstances require.

Recommendation R-2: The Board of Supervisors should consider the immediate need for additional funding to be provided both to County Counsel and the IT Department in order to improve existing and continuing compliance with California and Federal Privacy laws, rules and regulations. The CGJ believes funding at least one additional full time legal position for the County Counsel's office is imperative at this point, to help protect the County and its citizens. The IT Department also needs more funds to acquire and use various protective software packages that warn of impending attempts at data intrusion and stop them; and perhaps for one additional key person to head and direct the development and continuing maintenance of the County website on behalf of its many departments and agencies.

> ***Response R-2:*** This recommendation requires further analysis, in part, as the recommended allocation of resources must be consistent with overall County budget and competing priorities. This recommendation has been implemented in part. Funding for an upgrade to the County's intrusion detection systems and a next generation firewall has already been requested and has been obtained through the capital replacement program.

Recommendation R-3: County Counsel's office should promptly take all steps necessary to formally designate one of its lawyers as "County Privacy Law Counsel" and to provide for that person's continuing legal education in this extremely complex area of the law. This should include education to the point of certification of his or her knowledge in this field by the IAPP, the standard of this industry. We have been told portions of such proposed actions are currently underway.

> ***Response R-3:*** This recommendation will be implemented, in part, in that attorney(s) with the County Counsel's office will be undergoing training in the area of data security and privacy by the International Association of Privacy Professionals (IAPP). Portions of

this recommendation require further analysis as the need for "formal designation" of a title is uncertain.

Recommendation R-4: The duties of such Privacy Counsel should encompass working closely on a continuous basis with the IT Privacy Directors and County Department managers on *existing* and future Privacy Policies, and on all proposed contracts where vendors may have access to County records and on all software licenses with third-party vendors. Privacy Counsel also needs to monitor closely these ever-changing laws to be certain that when changes in such laws occur these modified legal obligations and requirements are promptly communicated to responsible County personnel; so that they can be reflected quickly in then existing Policies; and so that follow-up educational meetings can be made for County personnel who must comply with these new laws.

> ***Response R-4:*** This recommendation will be implemented as circumstances require. The attorney(s) who undergo IAPP training in the area of data security and privacy will monitor the applicable laws, will consult with county personnel on these issues, and will assist with educational efforts, as needed. Attorneys with County Counsel regularly consult internally regarding contracts in which vendors will have access to County records to perform contractual obligations and regarding software licenses.

Recommendation R-5: The County Information Technology Department Director and the Chief Security & Privacy Officer, working with the Security and Privacy Officers in other Departments, should be commended for the recent massive revision of Monterey County Privacy and Security Policies. This critical project has been on-going for more than for six years, in order to replace the existing, obsolete 2002-2004 versions. Unfortunately, these old Policies, as of May 2014, were still posted on the IT Department website, as well as a 2008 version which apparently still exists but is accessible only internally. In an effort to reduce County exposure for failure to comply with existing California and Federal Laws, and in fairness to Monterey County residents, prompt completion and dissemination of these revised Privacy and Security Policies should be a priority, especially since large amounts of Personally Identifiable Information ("PII") could otherwise be at risk of illegal disclosure.

> ***Response R-5***: This recommendation has been implemented. Posting the revised policies on the public website was completed shortly after their approval by the Board and replaced earlier versions.

Recommendation R-6: Finally, the CGJ strongly recommends that the subject of education about compliance by all County employees and their departments with California and Federal Privacy and Security laws be taken more seriously. We understand that existing County Policies call for such education efforts in the form of providing and requiring attendance at biennial educational programs. Several CGJ members actually attended the current educational program, which was well presented and current. However, employees from the highest to the lowest level of County government must be made to realize that, while these Policies, rules and laws may seem burdensome and inconvenient, failure to comply may not only result in loss of their jobs, but also in massive and punitive penalties and legal fees incurred by the County if any such

violations were to be litigated. This educational process is not an easy, nor inexpensive, task, but it must not be minimized.

Response R-6: This recommendation is being implemented. Much effort has been made to put together and teach a solid and entertaining data security awareness program. An online version of the course has been completed and it is integrated with the County's Learning and Development system. The County does not "minimize" the importance of education; rather, it supports continuing educational efforts in the area of data security and privacy. The Board has previously made data security training mandatory for County employees and, in response to the grand jury report, will re-emphasize the importance of this training to the County workforce