# *City of Albuquerque*

## Office of Internal Audit

SECOND FOLLOW-UP OF THE
PERSONABLE IDENTIFIABLE INFORMATION (PII) SECURITY ON
CITY SYSTEMS – CITYWIDE AUDIT
Report #22-18-103F
Date: December 15, 2021

### ***INTRODUCTION***

The Office of Internal Audit (OIA) issued Audit No. 18-103, Personable Identifiable Information (PII) Security on City of Albuquerque (City) Systems – Citywide on February 27, 2019. OIA issued the first follow-up report on March 11, 2021 and found that of the three recommendations made in the original report, two were fully implemented and considered closed and one remained in process. OIA completed a second follow-up to determine the corrective actions that the Technology & Innovation Department (Technology and Innovation) has taken in response to the one remaining recommendation and determined it has been fully implemented and is now considered closed. Audit recommendations that were determined to be previously resolved and/or fully implemented are not included in this follow-up report.

### ***BACKGROUND***

OIA completed a citywide performance audit of PII Security on City Systems for the audit period October 2, 2018 through January 23, 2019. This audit was included in OIA's fiscal year (FY) 2018 audit plan. The audit objectives were to determine:

- Does the City maintain an active listing of systems and devices that contain PII?
- Does the City have controls in place to classify and safeguard PII including intake points, release/data sharing points and storage?
- Are individuals with access to the City's computer environment trained on and aware of their responsibility to safeguard PII?

Further information pertaining to the audit scope, limitations, and methodology can be found in Appendix A of the original audit report.

The increase in security breaches involving PII throughout the country has contributed to the loss of millions of records over the past few years. Security breaches involving PII are harmful to both organizations and individuals. Organizational damages may include a loss of public trust, legal liability, or remediation costs. Individual damages may include identity theft, embarrassment, or blackmail. Technology and Innovation is responsible for monitoring the security of the City's PII.

### ***OBJECTIVE***

The objective of this second follow-up was to determine whether Technology and Innovation has taken the corrective actions recommended in OIA'S February 27, 2019 audit. Consistent with Government Auditing Standards, Section 9.08, promulgated by the U.S. Government Accountability Office, the purpose of audit reports includes facilitating a follow-up to determine

whether appropriate corrective actions have been taken. This field follow-up is a non-audit service. Government Auditing Standards do not cover non-audit services, which are defined as professional services other than audits or attestation engagements. Therefore, Technology and Innovation is responsible for the substantive outcomes of the work performed during this follow-up and is responsible to be in a position, in fact and appearance, to make an informed judgment on the results of the non-audit service. OIA limited our scope to actions taken to address our audit recommendation from the first follow-up audit report dated March 11, 2021 through the submission of actions on November 24, 2021.

## ***METHODOLOGY***

To achieve the objective, OIA:

- Obtained documentary evidence from Technology and Innovation.
- Interviewed Technology and Innovation to understand and verify the status and nature of the corrective actions taken.
- Verified the status of the recommendation that Technology and Innovation had reported as implemented.

## ***RESULTS***

The one remaining recommendation made in the original follow-up report has been fully implemented. Therefore, all three recommendations included in the original audit report have been implemented and are now considered closed. See ATTACHMENT 1.

PREPARED:

DocuSigned by:
Vanessa Meske
FEF77AB7F20B4DD...
Vanessa Meske, Principal Auditor
Office of Internal Audit

REVIEWED:

DocuSigned by:
Sarah Faford-Johnson
F50CB9721C59445...
Sarah Faford-Johnson, Contract Auditor
Office of Internal Audit

APPROVED:

DocuSigned by:
Marisa Vargas
0F462D006A1E4C8...
Marisa Vargas, Acting City Auditor
Office of Internal Audit

APPROVED FOR PUBLICATION:

DocuSigned by:
Edmund E. Perea, Esq.
645A1FA5A6314C3...
Edmund E. Perea, Esq.
Accountability in Government Oversight Committee Chairperson

ATTACHMENT - 1

| Recommendation | Responsible Department | Original Department Response | Second Follow-Up Department Response | OIA Conclusion | OIA Use Only Status Determination |
|---|---|---|---|---|---|
| Recommendation 2#:<br><br>DTI should:<br>Develop comprehensive policies and procedures for classifying and safeguarding PII. The policies and procedures should include:<br>• City departments' guidelines for classifying and safeguarding the intake, storage/disposal, and release/sharing of PII.<br>• Guidelines for handling a data breach that specifically address which regulations apply and who to notify depending on the type of data involved. Appendix C includes a PII Regulations Matrix that lists various regulations, the type of entity that may be affected by the regulation, what is determined to be PII, and what should be done in the event of a data breach.<br>• Review its current practices including IT | Department of Technology & Innovation (DTI) | The Department of Technology and Innovation agrees with this finding and the recommendations. | The Personally Identifiable Information and Sensitive Data Policy was reviewed and approved by TRC and ISC. The policy has been posted on the CABQ website (https://eweb.cabq.gov/tools/Pages/IT_PoliciesStandardsProcedures.aspx?PageView=Shared).<br><br>All City employees were notified of the policy via eWeb (https://eweb.cabq.gov/_layouts/15/listform.aspx?PageType=4&ListId=%7BBE5086FA%2D5234%2D4A1D%2DB413%2DCCFB37CCA48A%7D&ID=6804&ContentTypeID=0x01040068176D9F00B05540B46DABFBE0254AA0). At the beginning of all monthly ISGG Meetings the group is asked about any new PII items and or projects. | OIA verified in the first follow-up completed March 11, 2021 that DTI developed comprehensive policies and procedures that classify the safeguard of personal identifiable information (PII). The policies and procedures were approved by DTI Management and communicated to city employees before the end of the third quarter of fiscal year 2021.<br><br>OIA obtained a copy of the *Personally Identifiable Information and Sensitive Data Policy*, (approved March 24, 2021 by the Technical Review Committee), and confirmed the policy addresses guidelines for classifying and safeguarding the intake, storage, disposal, and sharing of PII.<br><br>Additionally, OIA obtained a copy of DTI's internal *"Steps for Addressing a Data Breach Incident"*, and confirmed it provides specific guidelines for DTI to notify the City's insurance company, through Risk Management, if a breach | ☐ Open<br>☒ Closed<br>☐ Contested |

| Recommendation | Responsible Department | Original Department Response | Second Follow-Up Department Response | OIA Conclusion | OIA Use Only Status Determination |
|---|---|---|---|---|---|
| functions maintained by City departments outside of DTI's main authority and develop citywide policies and procedures that address data breaches. | | | | is confirmed and has a significant impact. The outside Insurance company will then assign a lead expert to create a response plan and assist DTI with the applicable regulations and which external parties to notify based upon the type of data involved. | |

**APPENDIX C** **PII Regulations Matrix**

| Regulation | Responsible Entity | Applicable PII | Process for Data Breach |
|---|---|---|---|
| Health Insurance Portability and Accountability Act of 1996 (HIPAA) | **§ 160.103 Definitions.**<br>(3) Business associate includes:<br>(i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.<br>(ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity.<br>(iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate. | **§ 160.103 Definitions.**<br>Protected health information means individually identifiable health information:<br>(1) Except as provided in paragraph (2) of this definition, that is:<br>(i) Transmitted by electronic media;<br>(ii) Maintained in electronic media; or<br>(iii) Transmitted or maintained in any other form or medium.<br>(2) Protected health information excludes individually identifiable health information:<br>(i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;<br>(ii) In records described at 20 U.S.C.1232g(a)(4)(B)(iv);<br>(iii) In employment records held by a covered entity in its role as employer; and<br>(iv) Regarding a person who has been deceased for more than 50 years. | **§ 164.404 Notification to individuals.**<br>(a) Standard — (1) General rule. A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach. Except as provided in § 164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.<br>**§ 164.408 Notification to the Secretary.**<br>(a) Standard. A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in § 164.404(a)(2), notify the Secretary.<br>**§ 164.412 Law enforcement delay.**<br>If a law enforcement official states to a covered entity or business associate that a notification, notice, or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or business associate shall: (a) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or b) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described |

| | | | |
|---|---|---|---|
| | | | in paragraph (a) of this section is submitted during that time. |
| Family Educational Rights and Privacy Act (FERPA) | (Authority: 20 U.S.C. 1232g(b)(1) and (b)(2))<br>“Early childhood education program” means –<br>(a) A Head Start program or an Early Head Start program carried out under the Head Start Act (42 U.S.C. 9831 et seq.), including a migrant or seasonal Head Start program, an Indian Head Start program, or a Head Start program or an Early Head Start program that also receives State funding;<br>(b) A State licensed or regulated child care program; or<br>(c) A program that –<br>(1) Serves children from birth through age six that addresses the children's cognitive (including language, early literacy, and early mathematics), social, emotional, and physical development; and<br>(2) Is –<br>(i) A State prekindergarten program;<br>(ii) A program authorized under section 619 or part C of the Individuals with Disabilities Education Act; or<br>(iii) A program operated by a local educational agency.<br>“Education program” means any program that is principally engaged in the provision of | (Authority: 20 U.S.C. 1232g(b)(4)(A))<br>"Personally Identifiable Information" The term includes, but is not limited to--<br>(a) The student’s name;<br>(b) The name of the student’s parent or other family members;<br>(c) The address of the student or student’s family;<br>(d) A personal identifier, such as the student’s social security number, student number, or biometric record;<br>(e) Other indirect identifiers, such as the student’s date of birth, place of birth, and mother’s maiden name;<br>(f) Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or<br>(g) Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates. | (Authority: 20 U.S.C. 1232g(b)(4)(B), (f), and (g)) (c) If the Office finds that a third party, outside the educational agency or institution, violates §99.31(a)(6)(iii)(B), then the educational agency or institution from which the personally identifiable information originated may not allow the third party found to be responsible for the violation of §99.31(a)(6)(iii)(B) access to personally identifiable information from education records for at least five years.<br>(d) If the Office finds that a State or local educational authority, a Federal agency headed by an official listed in § 99.31(a)(3), or an authorized representative of a State or local educational authority or a Federal agency headed by an official listed in § 99.31(a)(3), improperly rediscloses personally identifiable information from education records, then the educational agency or institution from which the personally identifiable information originated may not allow the third party found to be responsible for the improper redisclosure access to personally identifiable information from education records for at least five years.<br>(e) If the Office finds that a third party, outside the educational agency or institution, improperly rediscloses personally identifiable information from education records in violation of § 99.33 or fails to provide the notification required under § 99.33(b)(2), then the educational agency or institution from which the personally identifiable information originated may not allow the third party found to be responsible for the violation access to personally identifiable information from education records for at least five years. |

| | | | |
|---|---|---|---|
| | education, including, but not limited to, early childhood education, elementary and secondary education, postsecondary education, special education, job training, career and technical education, and adult education, and any program that is administered<br>by an educational agency or institution. | | |
| Payment Card Industry Data Security Standard (PCI DSS) | PCI DSS applies to all entities involved in payment card processing—including merchants, processors,<br>acquirers, issuers, and service providers. PCI DSS also applies to all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD). | Cardholder Data includes:<br>• Primary Account Number (PAN)<br>• Cardholder Name<br>• Expiration Date<br>• Service Code<br><br>Sensitive Authentication Data includes:<br>• Full track data (magnetic-stripe data or equivalent on a chip)<br>• CAV2/CVC2/CVV2/CID<br>• PINs/PIN blocks | **12.10** Implement an incident response plan. Be prepared to respond immediately to a system breach.<br>**12.10.1** Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum:<br>• Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the<br>payment brands, at a minimum.<br>• Specific incident response procedures.<br>• Business recovery and continuity procedures.<br>• Data backup processes.<br>• Analysis of legal requirements for reporting compromises.<br>• Coverage and responses of all critical system components.<br>• Reference or inclusion of incident response procedures from the payment brands. |
| New Mexico Data Breach Notification Act | SECTION 8.<br>EXEMPTIONS. --<br>The provisions of the Data Breach Notification Act shall not apply to a person subject to the federal Gramm-Leach-Bliley Act or the federal Health Insurance Portability and | C. "personal identifying information":<br>(1) means an individual's first name or first initial and last name in combination with one or more of the following data elements that relate to the individual, when the data elements | SECTION 6. NOTIFICATION OF SECURITY BREACH. --<br>A. Except as provided in Subsection C of this section, a person that owns or licenses elements that include personal identifying<br>information of a New Mexico resident shall provide notification to each New Mexico resident |

| | | | |
|---|---|---|---|
| | Accountability Act of 1996. | are not protected through encryption or redaction or<br>otherwise rendered unreadable or unusable:<br>(a) social security number;<br>(b) driver's license number;<br>(c) government issued identification number;<br>(d) account number, credit card number or debit card number in combination with any required security code, access code or password that would permit access to a person's financial account; or<br>(e) biometric data; and<br>(2) does not mean information that is lawfully obtained from publicly available sources or from federal, state or local government records lawfully made available to the general public. | whose personal identifying information is reasonably believed to have been subject to a security breach. Notification shall be made in the most expedient time possible, but not later than forty-five calendar days following discovery of the security breach, except as provided in Section 9 of the Data Breach Notification Act.<br><br>B. Notwithstanding Subsection A of this section, notification to affected New Mexico residents is not required if, after an appropriate investigation, the person determines that the security breach does not give rise to a significant risk of identity theft or fraud.<br><br>C. Any person that is licensed to maintain or possess computerized data containing personal identifying information of a New Mexico resident that the person does not own or license shall notify the owner or licensee of the information of any security breach in the most expedient time possible, but not later than forty-five calendar days following discovery of the breach, except as provided in Section 9 of the Data Breach Notification Act; provided that notification to the owner or licensee of the information is not required if, after an appropriate investigation, the person determines that the security breach does not give rise to a significant risk of identity theft or fraud.<br><br>D. A person required to provide notification of a security breach pursuant to Subsection A of this section shall provide that notification by:<br>(1) United States mail;<br>(2) electronic notification, if the person required to make the notification primarily communicates with the New Mexico resident by electronic |

| | | | |
|---|---|---|---|
| | | | means or if the notice provided is consistent with the requirements of 15 U.S.C.<br>(3) a substitute notification, if the person demonstrates that:<br>(a) the cost of providing notification would exceed one hundred thousand dollars ($100,000);<br>(b) the number of residents to be notified exceeds fifty thousand; or<br>(c) the person does not have on record a physical address or sufficient contact information for the residents<br>that the person or business is required to notify.<br><br>E. Substitute notification pursuant to Paragraph (3) of Subsection D of this section shall consist of:<br>(1) sending electronic notification to the email address of those residents for whom the person has a valid email address;<br>(2) posting notification of the security breach in a conspicuous location on the website of the person required to provide notification if the person maintains a website; and<br>(3) sending written notification to the office of the attorney general and major media outlets in New Mexico.<br><br>F. A person that maintains its own notice procedures as part of an information security policy for the treatment of personal identifying information, and whose procedures are otherwise consistent with the timing requirements of this section, is deemed to be in compliance with the notice requirements of this section if the person notifies affected consumers in accordance with its policies in the event of a security breach. |

Source: Various regulations identified in table