Audit Report

DATA PRIVACY – HUMAN SERVICES

As of August 2013

Office of the Controller
County of Northampton
Pennsylvania

STEPHEN J. BARRON, JR., CFE

CONTROLLER OF NORTHAMPTON COUNTY
NORTHAMPTON COUNTY COURTHOUSE
669 WASHINGTON STREET
EASTON, PENNSYLVANIA 18042

PHONE (610) 559-3186
FAX (610) 559-3137

FRANK S. KEDL, CIA
Audit Manager

TIMOTHY P. BRENNAN, ESQ.
Solicitor

February 28, 2014

Members of the Northampton County Council
John A. Brown, County Executive
County of Northampton, Pennsylvania

We have completed an audit of Data Privacy Controls in the Department of Human Services as of August 2013.

The Executive Summary on page 1 summarizes the audit results, while the Audit Results section provides a detailed explanation.

We acknowledge the cooperation and assistance we received from all of the Divisions within the Department of Human Services and the County's Information Services Division. Their help was essential to the performance of this audit.

Our report was discussed with management at our exit conference on February 25, 2014. Management's response is included in the Audit Results section of the report.

Very truly yours,

Stephen J. Barron, Jr., CFE
County Controller

Anthony D. Sabino, CIA
Lead Auditor

Table of Contents

PAGE

EXECUTIVE SUMMARY

The Human Services Department is fully aware of the laws and regulations regarding the privacy of data collected from clients in the course of providing services. We found that all of the Divisions within this Department make every effort to comply with the various laws and regulations regarding data privacy. Employees are trained and periodically retrained to ensure they are fully aware of all of the requirements related to the custody of sensitive and private information. In our audit, we only found two minor areas where improvements might be made, but on the whole the Department protects private information and retains it only as long as they are legally required.

INTRODUCTION

One of the most challenging issues faced by businesses and governments today is the protection of private and sensitive information collected on both employees and clients. Data privacy breaches make headlines with increasing frequency, with the danger being that private information may be used for purposes other than originally intended.

Many Northampton County Government Departments collect private information in the course of their regular duties. The Department of Human Services includes a number of Divisions, such as Drug and Alcohol, Mental Health and Children and Youth which must accumulate sensitive and private information in order to treat their clients. This information must also be shared with certain third-party vendors.

The federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) sets national standards for the protection of health information for covered entities. The Northampton County Human Services Department is considered a covered entity under HIPAA, therefore the department is required to comply with all of the aspects of this law. In addition, some Divisions are subject to other privacy legislation, some of which are even more restrictive than HIPAA.

The County covers Data Privacy in two policies in the Employee Manual. The Code of Ethics policy specifically includes a section prohibiting the use of confidential information, and the Discipline policy includes the unauthorized release of confidential information as a violation for which discipline can be meted out.

Human Services conducts annual training on the requirements of HIPAA. All Human Service employees are required to attend. Also, employees in some of the individual Human Service divisions attend additional training on the various other applicable regulations. In addition to being cognizant of the applicable laws and regulations, employees in the Human Services Department must take active steps to protect the electronic and hard copy files which contain private information. The County's Information Services Department assists in this effort by ensuring that the County's electronic files are safe from outside infiltration.

PURPOSE AND SCOPE

The purpose of this audit was to ensure that an adequate level of security is maintained over private data collected in the Human Services Department.

The scope included all Human Service Divisions, as well as a review of County-wide policy and actions taken by the County's Information Services Department to protect electronic private data.

METHODOLOGY

In 2009, the AICPA issued a publication entitled "Generally Accepted Privacy Principles" which provides helpful guidance for auditors evaluating an organization's privacy program. This guide is used as a benchmark to provide useful information to management and is broken down into ten principles. In 2006, the Institute of Internal Auditors issued a Global Technology Audit Guide entitled "Managing and Auditing Privacy Risks" which provides additional guidance to the auditor performing reviews of privacy programs. Both of these guides were helpful in the completion of this audit.

In addition, we conducted interviews with all Human Services Division heads and other key employees with responsibility for implementing the privacy program.

We limited ourselves to a review of policies and procedures and did not conduct tests by reviewing individual electronic or hard copy files.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

AUDIT RESULTS

Section A – Internal Controls

1. Deletion of Electronic Backup Files

OBSERVATION

Each Division in Human Services is subject to a record retention schedule for both hard copy and electronic files. Older items are to be destroyed or purged. In our audit, we found that all Divisions destroy hard copy files on a timely basis, and that the Data Entry Division regularly purges electronic files.

Electronic files, however, are backed up daily and the backup media is stored at the Greystone Building. The backup files are not deleted when the source data is purged. In our conversations with a representative of our Information Services (IS) Division, we found that this data is stored in such a way that it is consolidated with other data, making specific files technologically impracticable or impossible to extract and destroy, while leaving other data intact. We inquired whether such data could be restored to the CareTracker software and, if so, would such information be discoverable in Court. This would negate the intent of the purge of the source data.

As of the end of fieldwork for this audit, the IS representative was attempting to obtain guidance from the State and the County Solicitor's Department as to whether retaining the backup files represents a violation of Record Retention Policies, and whether such data could be subpoenaed in a court case.

RECOMMENDATION

The IS Division should continue to work with the State and the Solicitor's Office to determine if retention of backup files after source data has been purged presents any legal issues.

MANAGEMENT RESPONSE – Allison E. Frantz, Director of Human Services

County of Northampton, IT Department is in process of developing a written policy specific to deletion of electronic backup files This policy will match the hard copy file record retention specifications, that is, back-files over 7 years old will be deleted. The IT Department is presently working with the County of Northampton's Solicitor's Office and other appropriate parties to determine if retention of backup files after source data has been purged presents any legal issues.

2. Business Associate Agreements

OBSERVATION

To comply with HIPAA, the Department of Human Services requires all third party vendors who have been provided access to Protected Health Information (PHI) by the County to complete a Business Associate Agreement. This document details the obligations of the third party with regard to the privacy of the information provided to them.

In our audit, we identified two vendors that have at least limited access to sensitive information, but no Business Associate Agreement had been obtained:

- Titan Mobile Shredding provides on-site shredding services to the Bechtel Building; Human Service employees deliver boxes of items to be shredded to the parking lot and Titan destroys them. However, the employees do not remain with the items as they are being shredded, so Titan has sole custody of this material for a brief period before it is destroyed.

- Similarly, Xerox employees have the ability to access electronic data within the CareTracker system without the presence of a Human Service employee. (It is not the policy of Xerox to access this information without the consent of a Human Service employee, but the technical ability does exist.)

Prior to the completion of our fieldwork, Human Services obtained a Business Associate Agreement with Titan, but the Agreement with Xerox had yet to be completed.

RECOMMENDATION

Human Services should continue to pursue the acquisition of a Business Associate Agreement with Xerox.

MANAGEMENT RESPONSE – Allison E. Frantz, Director of Human Services

The Human Services Business Associate Agreement with Xerox has been fully executed.