Mecklenburg County
Department of Internal Audit

County Manager's Office
Public Records Request–HIPAA Investigation
Report 1703

September 01, 2017

Internal Audit's Mission	To support key stakeholders in cultivating an environment of accountability, transparency, and good governance.
Internal Audit Contacts	Joanne Prakapas, CPA/CFF, CIA, CRMA, CFE, Audit Director (980) 314-2889 or joanne.prakapas@mecklenburgcountync.gov Christopher Waddell, CIA, CRMA, Audit Manager (980) 314-2888 or christopher.waddell@mecklenburgcountync.gov
Staff Acknowledgements	Eric Davis, CIA, CISA, CRMA, Auditor-In-Charge
Obtaining Copies of Internal Audit Reports	This report can be found in electronic format at http://charmeck.org/mecklenburg/county/audit/reports/pages/default.aspx

MECKLENBURG COUNTY
Department of Internal Audit

To: Dena Diorio, County Manager

From: Joanne Prakapas, Director, Department of Internal Audit

Date: September 01, 2017

Subject: Public Records Request–HIPAA Investigation Report 1703

The Mecklenburg County Public Information Department (Public Information) received public records requests from media outlet A and media outlet B on February 23 and February 27, 2017 respectively. These requests were for specific employee emails because of the disclosure that some patients who had received services at the Public Health Department had not been properly notified of abnormal Pap smear test results.

After the County Legal Department (County Legal) reviewed 1,454 emails and removed those containing personal and confidential information, such as PHI, the remaining emails were provided in digital versatile disc (DVD) form to media outlet B on March 20, 2017. Shortly thereafter, County management learned the released emails had several emails remaining with personal and confidential information and those were removed. Public Information staff redistributed a new updated DVD on March 27, 2017. On that same day, media outlet A asked for and was provided the DVD provided to media outlet B.

On March 27, 2017, media outlet A informed Public Information staff that PHI for County Health Department patients were included in the DVD they had just received. On March 28 and March 29, 2017, Public Information staff retrieved the DVDs from both media outlets. The County review calculated there were 2,041 records in total erroneously included. County Legal removed the PHI information, and new updated DVDs were redistributed on May 26, 2017.

On April 3, 2017, the Department of Internal Audit was asked to investigate the incident to determine whether there was intent to disclose PHI and to identify any control gaps that may have contributed to the disclosure. The investigation was limited to an evaluation of the Public Information, Information Technology (IT), and County Legal public records request processes for employee emails. Internal Audit interviewed key personnel; reviewed policies, procedures, and other documents; and observed operations.

CONCLUSION

There was no evidence to suggest the disclosure of PHI to the media was intentional, but rather due to human error. There was a failure of staff generating emails with protected information to mark it as protected information, as well as failure of staff to identify and remove protected information during the public request review process.

Our risk observations and recommendations for improvement, as well as management's risk mitigation strategies defined in Appendix A, are discussed in detail in the attached document. Internal Audit will conduct a follow-up review to verify management's action plans have been implemented and are working as expected.

We appreciate the cooperation staff provided during this investigation. Please feel free to contact me at 980-314-2889 if you have any questions or concerns.

c: Assistant County Managers
Deputy County Attorney
Senior County Attorney
Board of County Commissioners
Audit Review Committee
Human Resources Director
Chief Information Officer
Public Information Director

BACKGROUND

Per North Carolina General Statutes (NCGS) Chapter §132-1, any record created or received by county officials while conducting county business is considered public records and must be properly maintained and made available to the public upon request unless excluded by law. Public records include papers, letters, electronic documents, photos, videos, maps, computer files, and computer communications such as emails. Records are considered public unless they are exempt or otherwise protected by statutes and laws, such as NCGS §130A-12 and the Health Insurance Portability and Accountability Act (HIPAA). The HIPAA rules dictate how "covered" entities may use, disclose, and protect certain protected health information.

Privacy and Security Rules

To fulfill HIPAA requirements, the United States Department of Health and Human Services developed two rules commonly known as HIPAA Privacy and Security Rules.

- The Privacy Rule establishes national standards for protecting PHI, such as demographic information; medical history; and other data a healthcare professional collects to identify and provide patient care.
- The Security Rule establishes national standards for protecting PHI held or transferred in electronic form created, received, maintained, or transmitted in electronic form by a covered entity.

For purposes of HIPAA compliance, Mecklenburg County is a "hybrid" covered entity, which includes both covered and non-covered functions.

HIPAA Breach

A breach as defined by HIPAA is the "the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information." The United States Office of Civil Rights has jurisdiction over HIPAA breaches and may perform an investigation when a breach occurs to determine possible non-compliance with HIPAA Rules and fines and penalties a covered entity may incur.

Public Records Requests

North Carolina law requires a public records request be made to the records custodian at the specific department where the records are maintained. Further, County policy requires if protected information must be transmitted via email, the email should be appropriately marked as protected information. Any department-related processes should also be followed. Departments receiving a request should determine whether County Legal should first be consulted before fulfilling the request.

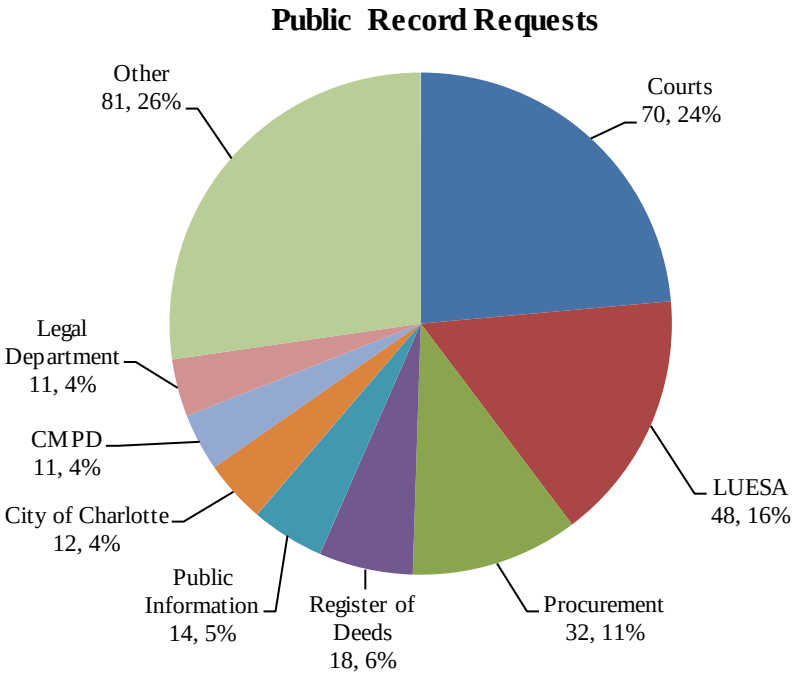
Other public records requests, such as requests for emails, must be submitted to Public Information in writing. If Public Information staff determines the request is routine, e.g., a vital records request, they will route the request to the appropriate County department or external state, federal, or local agency that has custody of the requested records and who is responsible for fulfilling the request.

For a non-routine public records request, Public Information staff determines whether the request should first be reviewed by County Legal to see if it meets the criteria for a public record. Although not documented in formal policy, all public records requests for employee emails are routed to County Legal for review.

County Legal receives the requested emails from Information Technology (IT) Security Services and conducts a detailed review to ensure no PHI or other personal or confidential information is included. Because email content cannot be redacted, any emails with such information must be deleted.

Once the review by County Legal is completed, the records are retrieved by IT Security Services staff who check to ensure the email "Deleted Items" box is cleared before burning the information onto a DVD. When the DVD is ready, Public Information notifies the requestor the records are ready to be picked up. Since this incident, however, County Legal has changed to a three-level review process to help mitigate the risk of unintentional disclosure of personal and protected information.

During January 1, 2016 – March 17, 2017, Public Information received 297 public records requests via the web portal, fax, and email.



Source: Mecklenburg County Public Information Department, unaudited

COUNTY MANAGER'S OVERALL RESPONSE

The County Manager concurs with all action plans and implementation timeframes.

RISK OBSERVATIONS AND MITIGATION STRATEGIES

1.1 **Policies and Procedures—**While there were formal, documented countywide policies and procedures for public records requests, some did not reflect current and/or best practices. Further, some departments did not have documented policies and/or procedures for administering public records request activities such as record keeping, record release authorization, and request monitoring and tracking. Yet, policies and procedures are important control activities to help management ensure its directives are carried out while mitigating risks that may prevent the organization from achieving its objectives.

Recommendation

1.1 Internal Audit recommends management update and develop as necessary formal, documented department-level and countywide public records request procedures. We further recommend management review and update as necessary all County public records request procedures to ensure a consistent approach across the organization to help mitigate the risk of unintentional disclosure of PHI or other personal or confidential information. Staff involved in the public request processes, including department management, should be trained accordingly.

The updated and new procedures should be consistent with applicable County policies and procedures, and include at a minimum:

- Key public records request process steps, e.g., request receipt and acknowledgement; record identification, collection, and release; criteria for record requests requiring County Legal review; supporting documentation maintenance; multiple layer attorney and other reviews; record release authorization; and request monitoring and tracking
- Staff roles and responsibilities
- Staff training requirements
- Periodic reviews and updates
- Internal and external communication requirements

Management's Response

1.1 **Risk Mitigation Strategy:** Reduce **Implementation Date:** December 2017

Action Plan: County legal, Information Security (ITS) and Public Information (PI) will work together to update current public records policy. ITS will finalize the public records request policy that addresses the handling of emails from a technical perspective. The RFP for software has been issued. The revised policy will address handling emails and e-Discovery. PI will reconfigure/redesign the online public records portal to better control processing records requests. County legal has revised the review process to now require a three (3) level attorney review for emails that potentially contain personal identifiable information (PII) or protected health information (PHI), which has been implemented. ITS along with PI has begun a temporary process

to document and track records requests until the new tool is implemented. This temporary process has been implemented.

2.1 **Public Records Request Tracking—**The County did not have a formal, consistent countywide process for tracking public records requests from receipt through final disposition. Therefore, management did not have the data to track the status of outstanding requests, effectively analyze the impact of responding to public records requests, and identify process efficiencies.

2.2 **Training—**While the County provides HIPAA training for staff, it does not require training on the public records request processes to ensure consistent application across the organization, which could increase the risk of violating public records law and HIPAA Rules.

Recommendations

2.1 Internal Audit recommends management create a formal tracking and monitoring process to capture and document public records requests received by the County. The process should capture at a minimum:

- The public records request method
- Requester name
- The date, time, and information requested
- The employee receiving the request
- All employees who work in the request
- All requester communications, including dates and times
- Request fulfillment method, e.g., paper, electronic media, etc.
- The number of records mailed, viewed, etc.
- Request deadline
- The resource cost to complete the request, e.g., employee hours spent on the request, as well as any cost recoveries

2.2 Internal Audit recommends management develop and extend public records request training to department management and all staff likely to encounter members of the public requesting public records, e.g., front-line staff who have daily contact with the public. At a minimum, the training should include parameters to help department staff understand what constitutes a public records request, which requests may include potential confidential or protected information, and when they should contact Public Information and/or County Legal before fulfilling a request.

Management's Responses

2.1 **Risk Mitigation Strategy:** Reduce **Implementation Date:** March 2018

Action Plan: Funds have been allocated to ITS and PI to identify and purchase an electronic tool to better handle processing of emails, e-Discovery and text messages. ITS has advanced a RFP to procure software for e-Discovery Solution Business requirements. The RFP requirements include formal tracking and monitoring of documents. It is to have the capability to provide reports from

the time of the request to the creation of document to final release including dates of activity/workflow/login/logout/routing status changes such as redactions, deletions etc. Among other things, the tool is to also have the capability to flag sensitive information in document and attachments such as personal identifiable information (PII), Criminal justice information (CJI), protected health information (PHI), social security numbers (SSN), and payment card information (PCI).

2.2 **Risk Mitigation Strategy:** Reduce **Implementation Date:** March 2018

Action Plan: As a component of the plan, the ITS and PI public records policy will also address employee training. This will include revising training modules to include information on North Carolina public records laws for staff who might handle public records requests.

APPENDIX A—Risk Mitigation Strategy Definitions

Risk Mitigation Strategy	Definition
Reduce	Risk response where actions are taken to reduce a risk or its consequences.
Accept	Risk response where no action is taken to affect the risk.
Transfer	Risk response where a portion of the risk is transferred to other parties.
Avoid	Risk response to eliminate the risk by avoiding or withdrawing from the activity giving rise to the risk.