Montgomery County Council

Committee: Directly to Council
Committee Review: N/A
Staff: Marlene Michaelson, Executive Director
Purpose: Receive briefing and have discussion – no vote expected
Keywords: #IGReport, data protection, access to records, inspector general investigation

AGENDA ITEM #4
October 27, 2020
Discussion

SUBJECT

Briefing – Office of Inspector General (OIG) Report Publication #21-003 – County SharePoint Exposes Sensitive Information of Vulnerable Populations

EXPECTED ATTENDEES

Megan Davey Limarzi, Inspector General
Fariba Kassiri, Deputy Chief Administrative Officer
Gail Roper, Director, Department of Technology Services (DTS)
Keith Young, Enterprise IT Security Office, DTS
David Godfrey, Chief Information Officer, HHS

DESCRIPTION/ISSUE

On September 24, 2020, the Inspector General sent a Memorandum of Investigation to then-Acting Chief Administrative Officer Richard Madaleno to advise him of the discovery of sensitive and Personally Identifiable Information found on information sharing platforms used by the County. She noted that OIG has raised concerns about data security issues several times in the last few years.

SUMMARY OF KEY DISCUSSION POINTS

The IG will brief the Council on the Office's report (see © 1-9) and Executive Staff will present their response to the 5 recommendations in the report and describe the actions they have taken thus far (see © 10-12). The OIG recommendations are as follows:

1. restrict access to the Tree House SharePoint site and associated files;
2. assess the extent to which the records of children evaluated by Tree House were accessed by persons without a need to know and take appropriate remediation measures;
3. discontinue the use of file sharing platforms until data security vulnerabilities are addressed;
4. alert County employees to the vulnerabilities existing with the County's use of document sharing platforms; and
5. instruct County employees and DTS to delete documents containing PII and other sensitive information from document sharing platforms.

This report contains:

Alternative format requests for people with disabilities. If you need assistance accessing this report you may submit alternative format requests to the ADA Compliance Manager. The ADA Compliance Manager can also be reached at 240-777-6197 (TTY 240-777-6196) or at adacompliance@montgomerycountymd.gov

MEMORANDUM OF INVESTIGATION

TO: Richard Madaleno
Acting Chief Administrative Officer

FROM: Megan Davey Limarzi, Esq.
Inspector General

DATE: September 24, 2020

SUBJECT: County SharePoint Platform Exposes Sensitive Information of Vulnerable Populations, OIG Publication #21-003

Regrettably, I am writing your office for the second time this year to advise of the discovery of sensitive and Personally Identifiable Information (PII) found on an information sharing platform used by the County. This is in addition to another advisement this year notifying of the discovery of non-public documents connected to County leadership and County departments on an information sharing platform. The Office of the Inspector General has in fact raised concerns with your office about data security issues several times in the last few years.

This most recent discovery involves the use of the SharePoint platform and among other things, the exposure of names, biographical data, medical information, clinician notes, and details of abuse of children evaluated by the Tree House Child Advocacy Center of Montgomery County Maryland, Inc. ("Tree House"). Tree House is a non-profit entitiy that contracts with the County to provide "medical evaluations, forensic interviews, ongoing mental health therapy, victim support and advocacy services, integrated care coordination, and other related services to a minimum of 700 child victims of sexual/physical abuse and neglect."[1] It appears that the information is available to any County employee or contractor that has access to the SharePoint platform.

Any actions the County may have initiated in response to my office's repeated concerns have not adequately addressed the vulnerabilities existing with the County's use of information sharing platforms. This latest example is by far the most serious exposure and in addition to potentially violating laws designed to protect the disclosure of sensitive and PII information, and perhaps Protected Health Information (PHI), poses a significant potential risk to those exposed and the County.

Background

On February 21 of this year, I notified your predecessor of a serious privacy risk involving the use of the Microsoft Office 365 application Delve, a built-in off the shelf collaboration tool. I explained that my office was able to access non-public documents connected to County

[1] Statement of work for contract #1100369, period of performance July 1, 2020 to June 30, 2021.

leadership and County departments through Delve. I reported that my office met with the County Chief Information Officer about the issue and she agreed to take immediate action to shore up related vulnerabilities.

At the time, my office spoke to a relevant Department of Technology Services (DTS) employee on several occasions to understand what they were doing to address the security vulnerability. The DTS employee reported that they were meeting with a team from Microsoft to work on the issue, including changing default permission settings and building training modules for employees. We observed no significant changes to Delve or increased communication with County employees about the vulnerabilities we reported.

On May 15 of this year, I again reported to your predecessor that my office found an unsecured document through Delve, but that the document contained PII. The document we found contained the social security number, date of birth, Medicare number, bank checking account number, bank savings account number, income and bank balance information, and applicant address for a Medicare benefits applicant. In that instance, we made recommendations directed to the DTS and the Department of Health and Human Services (DHHS) that if followed could have prevented this most recent exposure. We recommended the following:

- I strongly recommend the Department of Technology Services (DTS) notify County employees of the vulnerability with Delve, and instruct employees to examine their personal profiles and delete documents that contain sensitive information. Additionally, I recommend DTS conduct an assessment of shared document locations and delete those documents containing personally identifiable information.

- I further recommend that the County Department of Health and Human Services (DHHS) prohibit its employees from sharing documents containing sensitive information through unencrypted emails and document sharing sites; and that DHHS instruct all of their employees to examine personal profiles and shared locations and delete any documents that contain sensitive information.

On May 20, 2020, my office received information that the Risk Governance Committee discussed the OIG finding and "had an interest" in addressing the issue, but it's unknown what specific action was taken as a result of their interest.

On May 21, 2020, DTS announced to County Department Information Technology contacts (#MCG.Department IT) that they were "temporarily disabling the Delve feature within the County's Office 365 environment."[2] They explained that the action was being taken "so DTS and County Departments can complete file and SharePoint permissions remediation activities, provide user training, and establish adequate control mechanisms including the effort to develop a data classification roadmap."[3]

Although DTS started an initiative in August that involved DHHS aimed at improving security and management of SharePoint sites, the initiative appears focused on mapping, establishing groups, and assigning permissions, but it is unclear whether this effort will resolve restrictions

[2] Email from DTS to #MCG.Department IT, dated May 21, 2020
[3] Ibid

with individual documents. To my knowledge, DTS and DHHS seemingly chose not to follow our recommendation to delete or restrict documents containing personally identifiable information.

Furthermore, I am not aware of any action taken by DHHS to prevent the exposure of sensitive information through information sharing platforms or to educate and inform staff of the need for appropriate action.

On March 1, 2018, former Inspector General Edward Blansitt issued a report detailing findings related to the improper handling of a computer system data breach in 2016.[4] The report noted a "need for updated procedural and policy controls on access to information." The OIG report also cited a May 2017 Health Insurance Portability and Accountability Act (HIPAA) compliance audit overseen by the County Office of Internal Audit that found inadequate or outdated computer security policies and procedures. The report also mentioned that an IT security assessment conducted by the Gartner Corporation made recommendations "that might have prevented the incident."[5]

Inquiry and Outcome

On September 23, 2020, the OIG received information from a concerned County employee that they were able to access records pertaining to Tree House through the SharePoint platform. The employee explained that while searching for documents on a SharePoint site to which they had legitimate access, they received documents related to Tree House in their search results.

The employee stated that they reported the discovery to a DTS employee who was also able to access Tree House documents in the same manner. The DTS employee suggested that the employee contact the IT helpdesk.

The OIG followed the steps explained by the complainant and received 16 pages of search results (approximately 240 documents and files). Several of the documents were related to Tree House, but an even larger number were connected to other County Departments, including DHHS, Department of Finance, Department of General Service, DTS, and the Department of Transportation. A limited review of the documents and files pertaining to organizations other than Tree House revealed a variety document types, some containing sensitive information. For example, some documents pertaining to the Public Health Emergency Grant Program (PHEG) contained tax information and social security numbers of applicants.

With respect to Tree House, the OIG found a spreadsheet updated on September 22, 2020, containing the names, biographical data, medical information, clinician notes, and details of abuse of approximately 529 Tree House clients. We also found and were able to access "session notes" containing client names, biographical information, details of meetings with clients and family members. The "session notes" electronic files were titled with the client's name, date of interview, and what appears to be the reason for the interview.

[4] OIG Preliminary Investigation #18-001, Allegation of Improperly Handled Computer System Data Breach
[5] Ibid., page 1

Among the Tree House documents we were able to access; we also found several documents relating to administrative procedures and typed and handwritten staff meeting notes.

We are not detailing the specific steps we took to find the documents or providing screenshots of the data we found in order to minimize the possibility that someone could access the documents after reading our report. We will provide that information to whomever you direct to address this issue.

Recommendations

As a result of our findings, I recommend you:

1. restrict access to the Tree House SharePoint site and associated files;
2. assess the extent to which the records of children evaluated by Tree House were accessed by persons without a need to know and take appropriate remediation measures;
3. discontinue the use of file sharing platforms until data security vulnerabilities are addressed;
4. alert County employees to the vulnerabilities existing with the County's use of document sharing platforms; and
5. instruct County employees and the Department of Technology Services to delete documents containing PII and other sensitive information from document sharing platforms.

I strongly urge you not to delay in implementing the recommendations as the information described is still exposed and available to all County employees.

Please provide a response to this memorandum utilizing the attached response template by September 29, 2020. We will include any response we receive in the final issued memorandum and it will be made public as well.

cc: Fariba Kassiri, Deputy Chief Administrative Officer
Gail Roper, Chief Information Officer
Raymond Crowel, Director, Department of Health and Human Services

OIG Comments to the Administration's Response to OIG Publication #21-003:

The OIG provided the County's Chief Administrative Officer (CAO) an advance copy of this report and an opportunity to comment on the recommendations. A copy of the CAO's response in its entirety follows. We continue to be concerned that the response does not seem to fully grasp the severity of our findings or the impact of data exposure incidents to victims, including the County. The County's planned actions do not address the reality that documents containing PII and PHI are currently available to persons who have no legitimate need for them. The County's assertion that "vast swaths" of information stored on file sharing systems are not sensitive misses the point that even a single exposure incident can pose serious consequences to those involved.

As we note in this report, the OIG has reported on vulnerabilities with data security for several years, including two this year. To date, actions taken to address our observations have failed to ensure that County systems properly restrict access to sensitive information. The documents found during our investigation were created, posted, and or updated in the last few months, some were even updated the day before our discovery. Noted modifications implemented in April did not prevent us from finding documents in May or September. It is unclear how implementing a new "software tool to restrict access to files shared prior to March 2020" will address the availability of files created after March.

We acknowledge the quick actions taken since we first alerted the County to these vulnerabilities but are unwavering in our recommendations for more assertive actions while other steps are taken.

The Administration's Response to OIG Publication #21-003:

OFFICES OF THE COUNTY EXECUTIVE

Marc Elrich
County Executive

Richard S. Madaleno
Chief Administrative Officer

MEMORANDUM

TO: Megan Davey Limarzi, Esq.

FROM: Richard S. Madaleno, Chief Administrative Officer

DATE: September 29, 2020

SUBJECT: OIG Publication #21-003, County SharePoint Platform Exposes Sensitive Information of Vulnerable Populations

We thank the Office of the Inspector General for the notification regarding this critical matter. Below are our responses to the recommendations in your report.

Recommendation 1: Restrict access to the Tree House SharePoint site and associated files.

Response: We concur with the recommendation.

The Tree House Teams site and associated files were restricted on September 25, 2020.

Recommendation 2: Assess the extent to which the records of children evaluated by Tree House were accessed by persons without a need to know and take appropriate remediation measures.

Response: We concur with the recommendation.

A report of all accesses of the Tree House Teams site was run on September 25, 2020. Of the 44 people that accessed the site from July 1 through September 25, 16 were not involved in the investigation or working on the project. DTS is working with HHS and OCA to review that access logs of the 16 individuals and develop next steps. We will report back to you on the next steps by the end of this week.

101 Monroe Street • Rockville, Maryland 20850
240-777-2500 • 240-777-2544 TTY • 240-777-2518 FAX
www.montgomerycountymd.gov

Recommendation 3: Discontinue the use of file sharing platforms until data security vulnerabilities are addressed.

Response: Unfortunately, we are unable to concur with this recommendation.

Discontinuing the use of file sharing and collaboration across the County would drastically impact business operations, especially during a time of significant remote teleworking.

In April 2020, the Department of Technology Services (DTS) modified all file-sharing systems so that users must affirmatively indicate that the file can be shared with users. This modified the prior setting on the file-sharing systems that used "share with all users" as the default setting when new files are created in file-sharing systems.

Additionally, DTS is acquiring a software tool to restrict access to files that were shared prior to the March 2020 enterprise default file sharing reconfiguration. The software tool will allow DTS and departmental IT staff, in an easy and centralized manner, to find files that were shared too broadly and to quickly restrict access to those files. Files containing sensitive data will be prioritized first for remediation. This is a new tool that will be used for permissions oversight management. It provides both remediation and solutions going forward.

Vast swaths of information stored in County information systems, and by extension file sharing platforms, are not sensitive. (See for example the large amount of data posted to the County's open data website.) Requiring departments that do not handle sensitive information to suddenly stop use of file sharing platforms, which likely took months to create and implement based on business processes, would freeze unnecessarily ongoing business operations County-wide that do not involve any sensitive information.

In addition to technical steps being taken to mitigate the situation, please note that County users face serious repercussions if they mishandle inadvertently accessed sensitive information: all County users are subject to both the County's information security policy (Administrative Procedure 6-7) and the County's ethics law (Section 19A-15), which require users to keep confidential information that is not available to the public and to only access information as necessary in the performance of their official duties.

Recommendation 4: Alert County employees to the vulnerabilities existing with the County's use of document sharing platforms.

Response: We concur with the recommendation.

An Information Security Alert was sent to all users on March 4, 2020 discussing vulnerabilities of file sharing and recommendations of how to securely share files. A reminder Information Security Alert was sent to all users on September 28, 2020. In addition, my office distributed a separate message to the department and office directors and department IT contacts requiring their immediate attention and quick action to remediate access permissions on their department

Response to OIG Publication #21-003, County SharePoint Platform Exposes Sensitive Information of Vulnerable Populations
September 29, 2020
Page 3 of 4

SharePoint site. We have instructed all departments to complete their access permissions remediation by October 2, 2020.

Recommendation 5: Instruct County employees and the Department of Technology Services to delete documents containing PII and other sensitive information from document sharing platforms.

Response: Unfortunately, we are unable to concur with this recommendation.

Sensitive data is used throughout the enterprise for normal business operations. Discontinuing the use of file sharing and collaboration across the County would drastically impact business operations, especially during a time of significant remote teleworking.

As an alternative, the County is acquiring a software tool to restrict access to files that were shared prior to the March 2020 enterprise default file sharing reconfiguration.

On September 28, a notification was sent to department directors and department IT contacts instructing them to complete the remediation of access permissions by October 2. Additionally, a notice was sent to all users to remind them of the requirements in Administrative Procedure 6-7, including best practices in access control related to the County's file sharing technologies, that users may only access information necessary for the performance of their official duties, and that users must take steps to ensure that they know how to protect sensitive information consistent with applicable laws and County policies.

DTS will also be beginning a Process Re-engineering Data Initiative in the fourth quarter of 2020 to include the following business and technology re-engineering solutions:

1. Implementation of a software tool Varonis which provides the following:
    a. Varonis will scan enterprise data and monitor user activity on all County accounts.
    b. If any suspicious activity is found, Varonis can be used to lock down the files so that no malicious user can alter or damage data contained within those files.
    c. Varonis alerts on active threats as well, so if any employees within the organization try to access information that they are not authorized to access, they will be prevented from handling this data.
    d. Varonis also includes deep data inspection, a feature that enhances network protection through continuous monitoring and alerting.
    e. Varonis empowers system owners to understand the threat security classification system by looking at threat models that explain context and will help systems owners make threat assessments more accurately.
    f. The Varonis tool captures audit trail records in Microsoft Office 365 and on-premise Active Directory user activity, and alerts DTS to the changes that are happening on the system, such as unauthorized user activity and change control violations.
    g. It is also able to perform continuous risk assessments, which tracks our system's security health with predefined tools and dashboards that can be edited. As an example, you can highlight risks such as user passwords that never expire, or enabled system logins that should not be active.

Response to OIG Publication #21-003, County SharePoint Platform Exposes Sensitive Information of Vulnerable Populations
September 29, 2020
Page 4 of 4

2. The County acquired Advanced Threat Protection with the new Microsoft Enterprise Agreement. This will allow us to move forward with a user-defined data classification designation for sensitive data across all users in the enterprise. This functionality will give us the ability to protect non-public data and implement a major data classification effort. This initiative will be led by a new role within DTS, the Chief Data Officer.

Thank you again for alerting us to this serious issue. Ensuring the security of personally identifiable information, and of sensitive data at large is a top priority and these cracks will be corrected immediately.

cc: Fariba Kassiri, Deputy Chief Administrative Officer
Gail Roper, Director, Department of Technology Services
Raymond Crowel, Director, Department of Health and Human Services
Marc Hansen, County Attorney, Office of the County Attorney
Erin Ashbarry, Associate County Attorney, Office of the County Attorney
Keith Young, Enterprise Information Security Official, Department of Technology Services

OFFICES OF THE COUNTY EXECUTIVE

Marc Elrich
County Executive

Richard S. Madaleno
Chief Administrative Officer

M E M O R A N D U M

October 22, 2020

TO: Marlene Michaelson, Executive Director
Montgomery County Council

FROM: Richard S. Madaleno, Chief Administrative Officer for

SUBJECT: Montgomery County Council Session on OIG Publication #21-003, County SharePoint Platform Exposes Sensitive Information of Vulnerable Populations

On September 24, 2020, the Inspector General alerted us that Personally Identifiable Information was found on an information sharing platform used by the County. We understand this in an incredibly serious matter and took immediate action to remediate the security issues that have been discovered. In advance of the Council session on OIG Publication #21-003 on October 27, 2020, we are providing you a summary of the IG's recommendations and a summary of our actions.

IG Recommendation 1: Restrict access to the Tree House SharePoint site and associated files.

Response: We concur with the recommendation and the Tree House Teams site and associated files were restricted on September 25, 2020.

IG Recommendation 2: Assess the extent to which the records of children evaluated by Tree House were accessed by persons without a need to know and take appropriate remediation measures.

Response: An investigation into the access of records continues. Further details on the status of the investigation will be provided at a later date.

IG Recommendation 3: Discontinue the use of file sharing platforms until data security vulnerabilities are addressed.

Response: We are unfortunately unable to concur with this recommendation. Discontinuing the use of file sharing and collaboration across the County would drastically impact business operations, especially during a time of significant telework. Instead, the County must continue using file sharing while implementing appropriate safety measures to prevent exposure of sensitive data to other users in the County.

We have implemented the following safety measures across each of the Microsoft Office 365 file sharing and collaborative technologies:

- SharePoint Security Re-architecture - In early May, the County began a SharePoint security re-architecture project to standardize and clean up user access across all SharePoint sites in the County. On September 28, a notification was sent to department directors and department IT contacts instructing them to complete the remediation of access permissions in early October. As of October 21st, the County has completed the security re-architecture of 12 departmental SharePoint sites and 26 departmental sites are currently being cleaned up, with most of them being near completion.

- Groups/Teams Restrictions - To prevent new Groups from being created without any oversight, the County will be instituting a governance process to restrict who can create a new Group or Team to prevent accidental sharing of sensitive files. This process will be implemented prior to October 30th. In addition, a review of over 1,200 existing public Groups sites is being performed to determine if sensitive data exists on these sites. If sensitive data is found, the site will be immediately restricted.

- OneDrive Access Control - In March 2020, the County changed the default enterprise file sharing settings to a more restrictive setting. However, thousands of files exist which were shared across the organization. The County has purchased an automated tool to assist in restricting access to both sensitive and non-sensitive files. This effort is discussed in more detail below.

IG Recommendation 4: Alert County employees to the vulnerabilities existing with the County's use of document sharing platforms.

Response: We concur with the recommendation. An Information Security Alert was sent to all users on March 4, 2020 discussing vulnerabilities of file sharing and recommendations of how to securely share files. A reminder Information Security Alert was sent to all users on September 28, 2020. DTS is closely working with departments to limit access to sensitive data in SharePoint and providing me with a daily updates on the status of this effort.

IG Recommendation 5: Instruct County employees and the Department of Technology Services to delete documents containing PII and other sensitive information from document sharing platforms.

Response: Unfortunately, we are unable to concur with this recommendation. Sensitive data is used throughout the enterprise for normal business operations. Discontinuing the use of file sharing and

collaboration across the County would drastically impact business operations, especially during a time of significant telework.

As alternatives to deleting documents containing PII and other sensitive data, on October 19th the County acquired and installed a software tool to restrict access to files that were shared prior to the March 2020 enterprise default file sharing reconfiguration. Additionally, in August 2020 the County signed a revised Enterprise Agreement with Microsoft that includes many additional security features that the County will be implementing.

We have procured the Varonis software to assist in the remediation and discovery of unauthorized activity in our sharing platforms. The software is currently installed and actively monitoring our shared platforms. Varonis is the industry-leading tool for access control management and user monitoring. It provides the following services:

a. Varonis scans enterprise data and monitors user activity on all County accounts within Office 365.
b. The Varonis tool then classifies the sensitivity level of any data based on its contents. It then can assist with restricting access to any files based on hundreds of different configurable reports.
c. If any suspicious user activity is found, Varonis can be used to lock down the files so that no malicious user can alter or damage data contained within those files.
d. It is also able to perform continuous risk assessments, which tracks our system's security health with predefined tools and dashboards that can be edited. As an example, you can highlight risks such as user passwords that never expire, or enabled system logins that should not be active.

The County has also acquired Advanced Threat Protection with the new Microsoft Enterprise Agreement. This will allow us to move forward with a user-defined data classification designation for sensitive data across all users in the enterprise. This functionality will give us the ability to protect non-public data and implement a major data classification effort. This initiative will be led by a new role within DTS, the Chief Data Officer.

Thank you again for allowing us to speak on this serious issue at the October 27 Council session. Ensuring the security of personally identifiable information, and of sensitive data at large is a top priority and these vulnerabilities are actively being corrected.

cc: Megan Limarzi, Inspector General
Fariba Kassiri, Deputy Chief Administrative Officer
Gail Roper, Director, Department of Technology Services
Raymond Crowel, Director, Department of Health and Human Services
Marc Hansen, County Attorney, Office of the County Attorney
Erin Ashbarry, Associate County Attorney, Office of the County Attorney
Keith Young, Enterprise Information Security Official, Department of Technology Services
David Godfrey, Chief Information Officer, Department of Health and Human Services