Agenda Action Form Overview

The Board is requested to enter into a contract with Carolinas IT to conduct a HIPAA Privacy and Security Risk Assessment and a Gap Analysis. The contract amount is $52,160.00 and is available in Risk Management's Budget– Miscellaneous Contracts Line Item (102-422-0200-1601).

Background/Justification

What is HIPAA?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is Federal legislation that created national standards to protect the privacy of patients' medical records and other personal health information.

The HIPAA Privacy & Security Regulations give patients certain rights over their healthcare information. HIPAA also require certain Durham County departments to put policies and procedures in place to protect patients' health information, whether oral, written, or electronic, from being used by or disclosed to individuals not authorized to access it.

What organizations does HIPAA apply to?

HIPAA applies to covered entities. Covered entities are defined in the HIPAA rules as (1) health plans, (2) health care clearinghouses, and (3) health care providers that conduct certain health care transactions electronically. Generally, these transactions concern billing and payment for services or insurance coverage. Covered entities can be institutions, organizations, or persons.

HIPPA allows covered entities to designate themselves as hybrid entities. A hybrid entity is one that performs both covered and non-covered functions as part of its business operations. A covered function is any activity that a department performs that would cause the department to qualify as a covered entity. For example: Durham County is a hybrid entity[1] that has covered departments and non-covered departments. Departments such as EMS and Public Health are covered entities, while the tax department is not a covered entity. The Hybrid designation allows Durham County to focus HIPPA compliance efforts on covered departments like EMS and Public Health while allowing Durham County to refrain from imposing HIPAA compliance on non-covered departments like Tax.

Why conduct a Risk Assessment and GAP Analysis?

HIPAA risk assessments are a cornerstone of an effective HIPAA security program in properly securing electronic Protected Health Information (ePHI). Per federal regulations, Durham County Government (being a hybrid entity) is required to conduct an accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of the electronic protected health information it holds.[2] Identification of the County's current risks and vulnerabilities enables the County to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level[3]; and to implement security measures to guard

[1] Please see attachment: Durham County Declaration of Hybrid Entity Status.
[2] 45 C.F.R. 164.308(a)(1)(ii)(A).
[3] 45 C.F.R. 164.308(a)(1)(ii)(B)

against unauthorized access to ePHI[4]. The HIPAA Risk Assessment will focus on several departments, including Public Health, IS&T, EMS, Criminal Justice Resource Center, and DSS.

The Chief Information Security Officer and the Compliance and Privacy Officer has also included a County-wide GAP analysis, that goes beyond merely HIPAA compliance, to address the overall information security and privacy needs within Durham County Government. The framework used in this initiative will be the National Institute of Standards and Technology (NIST) 800-53, a component of the Federal Department of Commerce.

The primary goals of this initiative will be:

- Provide a baseline of the current state of information privacy and security practices.
- Identify compliance and security gaps that may be a risk to the County.
- Formulate risk mitigation strategies county-wide.
- Ensure the County appropriately protects the confidential information of citizens, employees, and business partners.

The GAP analysis will be conducted in FY2018 and will be contracted within the County Attorney's Office's-Risk Management Division. Stakeholders County-wide will be identified to participate in the analysis to ensure it holistically addresses information privacy and security risks. During the project kickoff, County Directors will be asked to identify one or more staff who can provide information on the department's overall business functions, internal policies, procedures, and processes. Funding for this initiative will come from the County Attorney's Office (Risk Management). The outcomes from this project will be used by the Chief Information Security Officer and the Compliance and Privacy Officer to work to meet the goals of this initiative.

Importance of compliance to HIPAA?
It is critical for covered entities and their workforce members to follow HIPAA's guidelines and requirements. Depending on the type and nature of a HIPAA violation, civil or criminal penalties may include devastating fines of up to $1.5 million per year or even imprisonment for up to 10 years. This is why Durham County Government should be certain that its overall systems and processes are handled in a HIPAA compliant manner.

Policy Impact
All work will be conducted to ensure Durham County Government's compliance with The Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended, and NIST 800-53.

Procurement Background
16 November 2017 – Durham County Government advertised RFP No. 18-012.

19 December 2017 – The Durham County Compliance and Privacy Officer and Evaluation Team received the vendors' bid packages from Purchasing and reviewed them.

[4] 45 C.F.R. 164.312(e)

11 January 2017 – Evaluation Team discussed bids received and requested that both vendors come in to interview.

7 February 2018 – Interviews were held for the two vendors that bid on RFP 18-012. Interview team consisted of Public Health's Privacy Officer, Public Health's Security Officer, Chief Information Security Officer, Public Health's IT Director, Durham County's Compliance and Privacy Officer, Chief Information Security Officer, Information Technology Manager, and the Assistant Director of IS&T. Carolinas IT had the lowest bid and was selected for the project.

Type of purchase

- ☐ Goods
- ☒ Services
- ☐ Architect, Engineer or Surveyor Services
- ☐ Construction and Repair

Did this request for purchase go through a bid process? Yes ☒ No ☐

Goods: Bids required if ≥ $30,000, BOCC approval if ≥ $90,000
Services: Bids required if ≥ $30,000, BOCC approval if > $40,000
Construction/Repair work: Bids required if ≥ $30,000, BOCC approval if ≥ $500,000

If yes, attach a copy of bid tab and the minority and women business enterprise (MWBE) compliance review form provided by the Purchasing Division.

Fiscal Impact

The total cost of the HIPAA Privacy and Security Risk Assessment and a Gap Analysis is $52,160.00.

Recommendation

It is recommended that the Board enter into a contract with Carolinas IT to conduct a HIPAA Privacy and Security Risk Assessment and a Gap Analysis. The contract amount is $52,160.00 available in Risk Management funds – Miscellaneous Contracts Line Item (102-422-0200-1601).