Isiah Leggett
County Executive

Leon Rodriguez
County Attorney

OFFICE OF THE COUNTY ATTORNEY

MEMORANDUM

TO: Keith Young, Department of Technology Services
Barbara Garrard, Department of Technology Services

FROM: Richard H. Melnick, Associate County Attorney
Karen L. Federman Henry, Division Chief

DATE: August 13, 2007

RE: Advice of Counsel—Data Security Issues

In the course of preparing for several projects, you encountered questions that required legal advice. This memorandum addresses the issues preliminarily. As you proceed through your tasks, additional information may require updating these responses, but this should give you a start toward handling your assignments.

1. Who is legally responsible for risk and privacy/security incidents? How does IPAC and Montgomery County Code Division 11D, DTS § 2-58D play into this?

The answers to these questions depend on the type of information and circumstances. An employee may be responsible directly, a supervisor may be responsible based on oversight, or the County may be responsible based on an established policy, practice, or procedure. Moreover, the County requires the placement of language in its contracts that imposes the same compliance standards on contractors who have access to County information and systems as those that apply to County employees. (*See* AP 6-7.) Procurement contracts also typically include indemnification and insurance language that addresses damages that may result from a contractor's breach of a contractual obligation to protect the security and privacy of County information or technology.

As you know, the Montgomery County Code identifies the functions and duties of DTS, and establishes the responsibilities of the Chief Information Officer (CIO). Montg. Co. Code §2-58D(a) and §2-58D(c) (2004). The law also delineates the obligations of the Information Technology Policy Advisory Committee (ITPAC). Montg. Co. Code §§2-58D (a) through (d).

To achieve its many purposes and duties, DTS employees, agents, and independent contractors must perform tasks that present countless security and privacy challenges while

ensuring the security and privacy of the County's sensitive information concerning its data and systems. As a starting point, DTS should identify all applicable policies, and maintain ready access to the administrative procedures and executive regulations that have been promulgated to govern the activities of those employees, agents, and contractors implementing the law on its behalf. When those procedures and regulations are modified or replaced, DTS must continue to ensure compliance with the new standards.

The relationship between the Director of DTS, the CIO, and ITPAC becomes crucial to ensuring consistency and adherence to the County's policies and procedures. The CIO acts under the supervision of the Chief Administrative Officer's (CAO) and also serves as chair of ITPAC. Additional responsibilities include review and approval of proposed procurement of information technology (subject to appeal by the Director of Procurement); managing major information technology projects under written policies approved by the CAO; providing technical assistance to ITPAC; and serving as the County liaison with other governmental agencies to promote efficient, practical, and consistent standards and operability of information technology in the County. Montg. Co. Code, §2-58D(c). Meanwhile, ITPAC includes a cross-section of agency heads and oversees the information technology policies and standards of the County government. Like the CIO, ITPAC seeks to: promote the efficient delivery of services to the public; promote interoperability with other public and private information technology systems; ensure the accuracy, integrity, and security of County information; and comply with federal, State, and local law. Both the CIO and ITPAC seek to ensure the efficiency, security, and privacy of the County's information systems and related data, and they must work collaboratively to satisfy their respective responsibilities.

2. What are the legal liabilities for those responsible above? How are these people protected from the (possibly personal) liabilities?

Employees may be sued for a variety of reasons while conducting the business of the County. Under State law, known as the Local Government Tort Claims Act (Md. Code Ann., § 3-501 *et seq.*), the County, a local government, must provide a defense for its employees (and in some cases, volunteers) in any action that alleges "damages resulting from tortious acts or omissions committed by an employee within the scope of employment with the local government." The law also requires the County to indemnify the employee for any judgments that might result. The County maintains a self-insurance fund to defend itself and its employees against these claims. The coverage includes the defense of the claim and payment of all judgments and settlements for damages resulting from the conduct described above. There is an exception in the law—the County is not required to pay for punitive damages imposed against an employee, so the employee may be liable for punitive damages. This type of damage results from a finding by a jury that the employee acted with malice (ill will or improper motivation) or acted outside the scope of employment. If an employee acts outside the scope of employment, a

defense of the claim also may be lost. Generally, unless the employee acts maliciously or outside the scope of employment, the County will defend the employee and pay any damage claims in a settlement or as the result of a judgment.

Additional potential liability may occur through the agency principles described in our previous memorandum to you. There we explained that the definition of an agent of the County often depends upon the facts and circumstances presented. Generally, an agent may bind his principal only to the extent that he has actual or apparent authority. *Progressive Casualty Insurance Company v. Ehrhardt*, 69 Md. App. 431, 440, 518 A.2d 151, 155 (1986) (citations omitted). In the absence of actual authority, an agent may have apparent authority only if the principal knowingly allows the agent to act for him and the agent induces a third party to rely on that authority. *Homa v. Friendly Mobile Manor, Inc.*, 93 Md. App. 337, 360, 612 A.2d 322, 333 (1992) (citing *Progressive, supra*). The agent's action or statement does not enlarge his own authority—only the principal's action or inaction affects the agent's authority. *Id.* at 363, 612 A.2d at 334-335. As we indicated previously, the clearest mechanism to establish the agency relationship is through a contract, which should specify the scope of the agent's authority and the precise duties included in the actual authority. Employees may serve as an agent of the County for certain matters, but even that relationship usually must be evaluated on a case-by-case basis: employees who act outside the scope of their employment would not usually be agents.

More often, a governmental entity cannot have an obligation imposed upon it to expend public funds without a formal decision to do so. In fact, when dealing with officers and agents of a municipality, people are charged with knowing the nature of the employee's duties and the extent of their powers. This often is viewed as preventing an employee from binding the County based on apparent authority. *See Alternatives Unlimited, Inc. v. New Baltimore City Board of School Commissioners*, 155 Md. App. 415, 843 A.2d 435 (1996). Nevertheless, caution is advisable when considering the extent of an employee's or contractor's authority.

Finally, there may be situations that create liability based on state or federal law. For example, medical information must be protected in accordance with HIPAA. (*See* 45 C.F.R. Parts 160 and 164). Generally, protected health information (PHI) can be used, communicated, shared, and disclosed between businesses that provide a service to the subject of the record (such as treatment, payment for services or for health care operations of the treatment provider) without the need for an informed consent from the subject of the PHI. There may be a need to negotiate and sign a qualified service integration agreement (QSIA) or a business associate agreement (BAA) between the service provider and the County. Where the confidential/personal information about a subject pertains to alcohol or other drug data (AOD), under 42 C.F.R. Part 2, the only way to share, disclose, use, or communicate information about the subject between businesses is through an informed consent that is signed by the subject of the record. The County requires all recipients of medical, alcohol, and substance abuse services to sign a Notice

of Privacy Practices (NOPP) document, which informs the recipients of these services of the County's use and disclosure obligations pertaining to PHI and AOD information. A multi-party consent form is also being developed that would make the record available for use/disclosure by the County under the conditions and circumstances described in the NOPP.

3. Do we have boilerplate legal documents with sanctions, such as non-disclosure agreements, employee background check approvals, and confidentiality/monitoring statements?

Departments that routinely conduct background checks prior to employment may have standard forms that they use. You may want to check with the Office of Human Resources for samples. Procurement contracts involve some basic forms that are useful and require certain boilerplate language for non-disclosure of information. Also, some public safety positions require background checks, as do some positions identified by State law. (*See* Md. Ann. Code, Family Law § 5-561(b)(9) requiring background checks of recreation center employees.) In particular, AP No. 6-7 is instructive. (*See* attached.)

This Office often works with departments on an issue-by-issue basis to address the needs of the particular agency and the circumstances of the case. Among the materials you provided to us are several that you may find useful for the monitoring language. (*See* AP Nos. 6-1, 6-6, 6-7, and 8-2.) In addition, this Office assists DTS in drafting non-disclosure/confidentiality agreements, which vary depending on the purpose for which they are used. (*See* attached sample.)

With our previous memorandum, we provided you copies of two opinions discussing employee background checks. The gist of the memoranda were that, under state law, the County must conduct a CJIS criminal background check for certain classes of employees, including those that provide IT support for the CJIS system itself. Other employees that the County must check include police, fire, corrections, individuals who work with minors, and taxicab operators. Although state regulations authorize a local government to conduct CJIS criminal background checks for all employees during the hiring process, the County does not broadly conduct checks on all new hires. Finally, some departments and agencies (DLC, Ride-On, Finance) conduct their own, more limited, non-CJIS criminal background checks through the use of credit reporting companies. Note that these latter types of background checks require the consent of the person.

4. Is the County required to archive certain electronic data for discovery purposes in case of lawsuits or other reasons? (See new Federal Courts discovery expectations.)

Each department should follow whatever policies are in place concerning the retention

and/or destruction of documents in the normal course (*e.g.* records retention and disposal schedule). County personnel are currently working on formalizing County-wide records management policies in this area. This project will include updating each agency's records retention and disposal schedule. However, once the County is on notice of a claim, or a lawsuit is filed, the County Attorney's Office will send the involved department a notice of preservation letter which will instruct the department to put a "hold" on any documents, electronic and paper, and any other evidence that may be related to the action, including electronic data in its original format. The preservation letter will describe the nature of the claim or lawsuit and advise generally what needs to be preserved. If there are any questions, personnel should contact the Litigation Division in the County Attorney's Office for any assistance. (*See* attached sample preservation letter—note that it is undergoing revision.)

5. When and how can IT personnel monitor/produce an employee's e-mail or other data for personnel actions and other investigatory issues?

Generally, the information accessed and stored on County computers by employees belongs to the County and, therefore, can be monitored or reviewed when there is a legitimate reason for the review. The applicable principles and standards appear in AP No. 6-1. (*See* attached.) Among the provisions of the administrative procedure is a requirement that both a department head and the CIO approve access to an employee's email or computer documents. As a practical matter, the department seeking the access usually will consult with the Office of the County Attorney if the situation involves a potential personnel action or other investigatory issue.

6. Who should DTS interface with to ensure that new proposed policies (such as the revised Security AP 6-7 and Incident Response Policy) conform to County Code?

The Office of the County Attorney provides legal advice for all agencies of the County. The attorneys assigned to advise DTS directly are Erin Ashbarry, Rich Melnick, and Karen Federman Henry. For some issues, the attorney assigned to advise the particular agency may provide assistance as well.

7. How do we ensure that contracts with third parties conform to the many laws and requirements including possible sanctions and termination clauses?

The procurement process includes conditions (both in the contract and in the general terms and conditions) that contractors comply with the laws that apply to the transaction. The contract administrator should monitor performance to ensure compliance and to address any errors as they occur. Sanctions and termination clauses also appear in contract documents. *See* Montg. Co. Code Ch. 11B; Montgomery County Procurement Regulations; and AP No. 6-7.

8. The Executive Branch of Montgomery County Government provides data services to other entities including the Legislative Branch (the Council), the Judicial Branch (the Courts), the State of Maryland (SAO), and even private citizens. How does the Executive Branch enforce its security policies on these independent entities? For instance, how could the Executive Branch sanction a judge who violates the security policy?

Several administrative procedures address these issues. (*See* for example AP Nos. 6-1, 6-6, 6-7, and 8-2.) As for enforcement with outside agencies, language similar to that contained in contracts could be included in a memorandum of understanding. Where the data sought pertains to HIPAA or 42 C.F.R. Part 2 (AOD) protected information, then the MOU or cooperating agency agreement must be accompanied by either a Business Associate Agreement or a Qualified Service Integration Agreement. The Business Associate Agreement is used when an outside entity is performing a function or activity on behalf of the County (a Covered Entity) or performing a service to a Covered Entity which involves use or disclosure of PHI. The Qualified Service Integration Agreement is used when the need arises to share PHI that includes AOD information between County agencies or departments. Additionally, the preliminary access screen could be modified to alert users to the ramifications of violating the security policies (currently there is an alert that it is a violation for an unauthorized user to access the system—this could be revised to address the additional issues).

The response to this inquiry may benefit from any additional information you can provide. Sometimes the terms and conditions of a contract address the sanctions that we can impose, while the circumstances in other instances may allow a personnel action, criminal charges, or discontinuation of the use as appropriate sanctions.

Endnote

We hope this provides you with a useful preliminary response to your questions. As you work with this information, please let us know of any additional questions or concerns you have.

Enclosures