ALAN WILSON
ATTORNEY GENERAL

August 9, 2013

The Honorable Gary Watts
Richland County Coroner
P. O. Box 192
Columbia, South Carolina 29209

Dear Coroner Watts:

Attorney General Alan Wilson has referred your letter of April 10, 2013 to the Opinions section for a response. The following is our understanding of your question presented and the opinion of this Office concerning the issue based on that understanding.

Issue (as quoted from your letter): *[If] Richland County Information Technology employees have access to our case files through their upkeep and maintenance of our computer program... is this a violation of HIPAA for them to be able to view our protected information from any computer through the county VPN and if so, what does the Information Technology Department need to do to correct this?*

Short Answer: As far as our opinion on how the law reads, this Office is not aware of maintenance of computer programs to be a HIPAA violation as long as any such maintenance is in compliance with the HIPAA laws. However, this Office would suggest you look to DHHS (the Department of Health and Human Services) for further guidance on and interpretation of HIPAA.

Law/Analysis:
As your question regards HIPAA, this Office has previously stated:

> HIPAA is the Health Insurance Portability and Accountability Act of 1996, 110 Stat. 1936 (1996), and was enacted to protect the privacy of health information. Regulations were promulgated by the Department of Health and Human Services regarding the privacy standards of medical records. 45 C.F.R. parts 160 and 164. As indicated in United States v. Sutherland, 143 F.Supp. 2d 609 (W.D.Va. 2001), HIPAA regulations establish the circumstances under which patient medical records may be revealed by health plans, health care clearinghouses, and most health care providers. As noted in an opinion of the Arkansas Attorney General dated August 23, 2002, the regulations generally,
>
> > prohibit the disclosure by covered entities of protected health information without the required consent, authorization, or agreement; they require notice by covered entities of the use and disclosure of protected health information to the affected individual; they require covered entities to develop and implement privacy policies and physical standards to protect health information; they require the designation of a privacy officer within the

> covered entity who is to be responsible for the development and implementation of a privacy policy for the covered entity; they require the designation by covered entities of a contact person or administrative office who is to be responsible for receiving complaints concerning compliance with the privacy policy of the covered entity; and they require covered entities to impose sanctions upon members of the entity's workforce who fail to comply with the entity's privacy policies.

In United States v. Zamora, 408 F.Supp.2d 295, 297-298 (S.D.Tex. 2006), the court stated that

> [p]ursuant to HIPAA, individually identifiable medical information cannot be disclosed by covered entities without the consent of the individual unless disclosure was expressly permitted by HIPAA. 45 C.F.R. § 164.502. There are several instances where disclosure is permitted without authorization from the individual. 45 C.F.R. § 164.512. "A covered entity may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law." 45 C.F.R. § 164.512 (emphasis added). "Required by law" is defined as "a mandate contained in law that compels an entity to make a use or disclosure of protected health information and that is enforceable in a court of law." 45 C.F.R. § 164.103. "Required by law includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information...." Id. A disclosure made pursuant to § 164.512(a) must meet the requirements outlined in § 164.512(c), (e), or (f). 45 C.F.R. § 164.512(a)(2). Section 164.512(f) provides for disclosure of protected information for law enforcement purposes. 45 C.F.R. § 164.512(f). This section permits disclosures for law enforcement purposes to a law enforcement official as required by law, or in compliance with "(A) A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer; (B) A grand jury subpoena; or (C) An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law...." 45 C.F.R. § 164.512(f)(1)(ii).As an initial matter, pursuant to § 164.512(f)(1)(ii)(C), information sought must be relevant and material to the law enforcement inquiry, the request must be specific and limited in light of the information sought, and de-identified information could not be reasonably used. (emphasis added).

As noted above and as set forth in the referenced prior opinion of this office, exceptions exist as to these regulations. As set forth by 45 C.F.R. Section 164.512,

> A covered entity[1] may use or disclose protected health information without the written authorization of the individual...or the opportunity for the

[1] The term "covered entity" is defined by 45 C.F.R. § 160.103 as a "(1) a health plan; (2) health care clearinghouse. (3) a health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter." I presume the Facility would be included within such definition. The term "health care provider" is defined as a "provider of services (as defined in 42 U.S.C.A. § 1395(u), a provider of "medical and

> individual to agree or object...in the situations covered by this section, subject to the applicable requirements of this section. When the covered entity is required by this section to inform the individual of, or when the individual may agree to, a use or disclosure permitted by this section, the covered entity's information and the individual's agreement may be given orally.
>
> Consistent with such, a covered entity may disclose or use protected health information without the written authority of an individual in certain different situations.

Op. S.C. Atty. Gen., May 7, 2008 (2008 WL 2324802). There are only two required disclosures of protected health information (PHI). The two required disclosures are when an individual requests under their right to access and when DHHS needs the information for compliance with the Privacy Rule. 45 C.F.R. § 154.502(a)(2). Other disclosures of protected health information (PHI) are authorized pursuant to 45 C.F.R. § 164.506. Any use or disclosure of protected health information (PHI) not required by law must be authorized. Id.

The Office believes the Office of Coroner would be a public health authority since it is an authority of a political subdivision of the state pursuant to 45 C.F.R. § 164.501. It is understood that most any authority and almost all health care providers may have business contracts with third parties for security (physical and electronic), cleaning, or information technology (website, electronic storage and backup, etc.). HIPAA provides that business associates may use or disclose permitted health information only as permitted or required by its business associate contract or other arrangement pursuant to § 164.504(e). 45 C.F.R. § 164.502(1)(3). HIPAA says that a business associate must "make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request." 45 C.F.R. § 164.502(b)(1). Additionally, HIPAA says "a covered entity may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor." 45 C.F.R. § 164.502 (e)(1)(i). The requirements of a contract between a covered entity and a business associate must meet the requirements of 45 C.F.R. § 164.504(e)(2). Additionally, a business associate may disclose protected health information (PHI) to "a business associate that is a subcontractor and may allow the subcontractor to create, receive, maintain, or transmit protected health information on its behalf, if the business associate obtains satisfactory assurances, in accordance with 45 C.F.R. § 164.504(e)(1)(i)." 45 C.F.R. § 164.504(e)(1)(ii). Those assurances must be documented by means of a written contract or otherwise complies with HIPAA. 45 C.F.R. § 164.504(e)(2). Further instructions on administrative safeguards are found in 45 C.F.R. § 164.308ff.

Further, as quoted from the U.S. Department of Health and Human Services website,

> May a covered entity hire a business associate to dispose of protected health information?
>
> Answer:

---

other health services (as defined in 42 U.S.C.A. § 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business." 45 C.F.R. § 160.103.

> Yes, a covered entity may, but is not required to, hire a business associate to appropriately dispose of protected health information (PHI) on its behalf. In doing so, the covered entity must enter into a contract or other agreement with the business associate that requires the business associate, among other things, to appropriately safeguard the PHI through disposal. See 45 CFR 164.308(b), 164.314(a), 164.502(e), and 164.504(e). Thus, for example, a covered entity may hire an outside vendor to pick up PHI in paper records or on electronic media from its premises, shred, burn, pulp, or pulverize the PHI, or purge or destroy the electronic media, and deposit the deconstructed material in a landfill or other appropriate area.

http://www.hhs.gov/ocr/privacy/hipaa/faq/safeguards/577.html. This Office would presume that a website maintenance entity would have to comply with similar requirements.

Conclusion: This Office is not aware of maintenance of computer programs and websites to be a HIPAA violation as long as any such maintenance is in compliance with the HIPAA laws. However, this Office would suggest you look to DHHS (the Department of Health and Human Services) for further guidance on, and interpretation of, HIPAA. This Office is only issuing a legal opinion. Until a court or the legislature specifically addresses the issues presented in your letter, this is only an opinion on how this Office believes a court would interpret the law in the matter. If it is later determined otherwise or if you have any additional questions or issues, please let us know.

Sincerely,

Anita S. Fair

Anita Smith Fair
Assistant Attorney General

REVIEWED AND APPROVED BY:

Robert D. Cook
Solicitor General