DEPARTMENT OF HEALTH & HUMAN SERVICES
Voice - (404) 562-7886, (800) 368-1019
TDD - (404) 562-7884, (800) 537-7697
(FAX) (404) 562-7881
http://www.hhs.gov/ocr/

OFFICE OF THE SECRETARY
Office for Civil Rights, Region IV
61 Forsyth Street, S.W.
Atlanta Federal Center, Suite 16T70
Atlanta, GA 30303-8909

November 29, 2012

(b)(6),(b)(7)(C)

Ms. Andrea Wilson, RHIA, CIPP, CIPP/G
Ms. Vicki Bowman
VHA Privacy Implementation Coordinator
Information Access and Privacy Office- 10P2C1
Department of Veterans Affairs-Veterans Health Administration
810 Vermont Ave., NW
Washington DC 20420

Re: (b)(6),(b)(7)(C) vs. Bay Pines VA Medical Center
OCR Transaction Number: 11-130323

Dear (b)(6),(b)(7)(C) Ms. Wilson and Ms. Bowman:

On July 10, 2011, the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR) received a complaint from (b)(6),(b)(7)(C) alleging that Bay Pines VA Medical Center is in violation of the Federal Standards for Privacy of Individually Identifiable Health Information and/or the Security Standards for the Protection of Electronic Protected Health Information (45 C.F.R. Parts 160 and 164, Subparts A, C, and E, the Privacy and Security Rules), and the Breach Notification Rule Subpart D - Notification in Case of Breach of Unsecured Protected Health Information ("PHI") (45 C.F.R. §§ 164.400-164.414).

Specifically, (b)(6),(b)(7)(C), Complainant and physician assistant of CE, alleges that his ex-girl friend, (b)(6),(b)(7)(C) (nurse at Bay Pines VA Medical Center), used (b)(6),(b)(7)(C) social security number to alter his AT&T account. (b)(6),(b)(7)(C) claims he guards his SSN well and suspects that (b)(6),(b)(7)(C) must have obtained his SSN from his medical records. (b)(6),(b)(7)(C) complained to his employer, Bay Pines VA Medical Center, which provided accounting of his records showing that (b)(6),(b)(7)(C) accessed his records 55 times. (b)(6),(b)(7)(C) was suspended for 10 days. However, (b)(6),(b)(7)(C) alleges that Bay Pines VA Medical Center's own procedures state that a HIPAA violation should have led to (b)(6),(b)(7)(C) termination not just a suspension. These allegations could reflect violations of §§164.502(a), 164.514(d)(2), 164.528(b), 164.530(c)(1), 164.530(d)(1) and 164.530(d)(2), 164.530(e)(1), 164.530(f), 164.404(a) and 164.408 respectively.

Please note that 45 C.F.R. § 164.502(a) states, in part, that a covered entity may not use or disclose PHI, except as permitted by the HIPAA Privacy Rule. 45 C.F.R. §164.514(d)(2) states,

in part, that a covered entity must identify those persons or classes of persons, as appropriate, in their workforce who require access to protected health information to carry out their duties. 45 C.F.R. §164.528(b) states, in part, the covered entity must provide the individual with a written accounting that meets the requirements specified in this subsection, including the disclosures of protected health information. 45 C.F.R. §164.530(c)(1) states, in part, that a covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information. 45 C.F.R. §164.530(d)(1) states, in part, that a covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures. 45 C.F.R. §164.530(d)(2) states, in part, that a covered entity must document all complaints received, and their disposition. 45 C.F.R. §164.530(e)(1) states, in part, a covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart. 45 C.F.R. §164.530(f) states, in part, that a covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures. 45 C.F.R. §164.404(a)(1) states, in part, that a covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach. 45 C.F.R. §164.408 states, in part, that for breaches involving less than 500 individuals, the Act provides that a covered entity may maintain a log of such breaches and annually submit such log to the Secretary documenting the breaches occurring during the year involved.

OCR enforces the Privacy, Security and Breach Notification Rules, and also enforces Federal civil rights laws that prohibit discrimination in the delivery of health and human services because of race, color, national origin, disability, age, and, under certain circumstances, sex and religion.

OCR notified Bay Pines VA Medical Center of the complaint filed by Complainant. This notification, which is OCR's initial written communication with the covered entity about the complaint, described the acts that are the basis of the complaint. OCR's notification to Bay Pines VA Medical Center included a written request for the results of their review of the complaint's allegations. OCR also requested a copy of Bay Pines VA Medical Center's policies and procedures with respect to specific procedures relating to the handling of PHI belonging to their patients. Ms. Vicki Bowman, Program Specialist for VHA, responded to OCR's written request for information on behalf of the covered entity.

In the response, Ms. Bowman submitted copies of the requested policies and procedures that are the subject of the investigation, which are necessary for OCR to determine whether it is complying with the applicable provisions of the Privacy, Security and Breach Notification Rules. Ms. Bowman reports that based on its internal investigation that the original allegations did have merit in that (b)(6),(b)(7) did in fact accessed (b)(6),(b)(7)(C) medical record a total of 55 times according to the accounting of disclosures report. This access of (b)(6),(b)(7)(C) medical record took place even though there was never a treatment relationship between (b)(6),(b)(7) and (b)(6),(b)(7) Our analysis of the information gathered through our investigation discloses that the actions of (b) (b)(6), of Bay Pines VA Medical Center were not consistent with the internal policies and procedures related to the impermissible use of PHI and the safeguarding of PHI. An internal

investigation reveals that due to the impermissible access of (b)(6),(b)(7)(C) medical record, (b)(6),(b)(7)(C) would be subject to the sanctions in accordance to the VHA's internal policy.

OCR's analysis of the information gathered through our investigation reflect that there was not a violation of Bay Pines VA Medical Center's sanction policy and that the 10-day suspension that (b)(6),(b)(7)(C) received was in fact consistent with the time frame designated in the VHA's internal sanctions policy. In addition to properly sanctioning (b)(6),(b)(7)(C) Bay Pines VA Hospital took the following voluntary corrective measures to demonstrate its willingness to voluntarily comply with the citied provisions of the Privacy Rule: (a) The VHA filed a timely breach report in compliance with the reporting procedures in place for breaches affecting less than 500 individuals; (b) In light of the potential financial harm that the Complainant may have suffered due to the breach, the Covered Entity provided the Complainant with credit monitoring of all three major credit agencies; (c) The Covered Entity sanctioned (b)(6),(b)(7)(C) with a ten (10) day suspension in accordance to their sanctions policy. The Covered Entity also provided additional training to (b)(6),(b)(7)(C) and has documented all of these actions in her employment record.

Based on the foregoing, we have determined that the corrective action measures taken by Bay Pines VA Medical Center and VHA are sufficient to effectively resolve the issues raised by Complainant, and furthermore demonstrate VHA's willingness to voluntarily comply with the applicable provision of the Privacy, Security and Breach Notification Rules. As part of its investigation, OCR also reviewed the covered entity's internal policies and procedures applicable to §§164.502(a), 164.514(d)(2), 164.528(b), 164.530(c)(1),164.530(d)(1) and 164.530(d)(2), 164.530(e)(1), 164.530(f), 164.404 and 164.408 of the HIPAA Privacy and Breach Notification Rules. Our review of the same deems them to be compliant with the Privacy and Breach Notification Rules.

Therefore, OCR has determined that all matters raised by this complaint, at the time it was filed, have now been resolved through voluntary compliance actions of Bay Pines VA Medical Center. We are accordingly closing this case. OCR's determination as stated in this letter applies only to the allegations in this complaint that were reviewed by OCR.

Under the Freedom of Information Act, we may be required to release this letter and other information about this case upon request by the public. In the event OCR receives such a request, we will make every effort, as permitted by law, to protect the information that identifies individuals or that, if released, could constitute a clearly unwarranted invasion of personal privacy.

If you have any questions, please contact Anitra Moreland, Investigator, at (404) 562-7521 (Voice), or (404) 562-7884 (TDD).

Sincerely,

Ivy R. Belton

/Roosevelt Freeman
Regional Manager