



PRIVACY BREACH INVESTIGATION & RECOMMENDED ACTIONS – BEND MEMORIAL CLINIC (BMC)

SUBMITTED BY: CHRIS APGAR, CISSP **DATE:** INITIATED APRIL 7, 2009, FINALIZED: JUNE 10, 2009 **Incident:** Oncology Access and Use of BMC Medical Records

A. Incident Details:	
1. Date of Incident	Inconclusive – Potentially occurred between late September 2008 and February 27, 2009
2. Date of discovery of incident	Suspected February 19, 2009; confirmed February 27th
3. Date Incident was reported to the Entity's Privacy Official	February 27, 2009
4. Status of investigation (e.g., completed, estimated completion date, etc.)	BMC investigation concluded. CHC investigation is outstanding and may impact required mitigating action.
5. Recommended Additional Corrective Action	<ul style="list-style-type: none"> • Obtain sworn statement from Cascade Health Community (CHC) legal counsel or other appropriate party that all BMC patient data (electronic and non-electronic) inappropriately accessed and potentially further retained by CHC Cancer Care of the Cascades (CCC) has been destroyed or returned. • Request CHC impose appropriate sanctions for workforce members inappropriately accessing, viewing or otherwise using BMC patient data for any purpose other than pursuant to the BMC/CCC on-call agreement and the BMC business associate contract. This includes workforce members accessing patient records for "treatment, payment or healthcare operations" when such access violated the established on-call agreement and BMC's business associate contract which was executed with each CCC workforce member allowed access to BMC's electronic medical record (EMR). • Record the inappropriate disclosure in each affected patient disclosure accounting record. • Notify Category 2 and 3 patients of a security breach (similar to notification of Category 1 patients) for all patients CHC CCC cannot justify access was directly related to on-call patient treatment because the data inappropriately accessed included the patients' social

	<p>security numbers.</p> <ul style="list-style-type: none"> Review audit monitoring policy to reasonably ensure external access to BMC's EMR is appropriate. Such a policy should require periodic audits of both internal and external access to BMC's EMR.
B. Incident Description –	
1. General Description	<p>BMC entered into a documented on-call oncology coverage Agreement with CCC December 24, 2008 wherein access to BMC's electronic medical record was limited to use for call coverage only. The final language was written and presented to BMC by a senior CHC administrator for BMC approval. BMC so approved as requested. (See Attachment A.)</p> <p>Previous to the execution of the on-call Agreement, BMC's three employed physicians including Drs. Kornfeld and Boone, had been helping CCC's sole employed physician, Dr. Bill Martin, with on-call oncology coverage since late September 2008. (see Attachment A reference to existing informal call coverage agreement.) On October 17 and December 31, 2008 respectively, Drs. Kornfeld and Boone left BMC. On or about January 1, 2009, each started employment with CHC.</p> <p>In an effort to ensure patients cared for by Drs. Boone and Kornfeld did not experience an interruption in care upon their departure, BMC created a 24 hour delivery policy to deliver properly released paper medical records to CCC. The process was HIPAA compliant and followed standard medical office procedures, requiring a release and request for records transfer to be signed by the patient to ensure security and privacy. A special courier run to CCC was created just for this purpose.</p> <p>The purpose of the call coverage Agreement was to address patient needs after normal clinic hours from 5 PM – 8 AM. The Agreement included specific requirements and restrictions regarding access to BMC's EMR. It was written and finalized by CHC EVP Joe Smith. (See attached Exhibit) Upon the insistence of CCC physicians, all workforce members of their own identification were given on-call access. CCC justified the access by noting that staff often entered the on-call work of the night before when reporting to duty, relieving CCC physicians of the task. All CCC staff allowed access to BMC's EMR for call coverage purposes were required to enter into a business associate relationship (HIPAA required) with</p>

BMC and appropriate business associate contracts were executed with each workforce member in order to ensure the purpose of access was for call coverage and servicing the Agreement.

BMC was notified by a patient on February 19, 2009 that he had been informed that his care had been transferred to CCC. The patient indicated he had not transferred his care and he indicated he was told by a CCC workforce member repeatedly that he had made an appointment with CCC. The patient also indicated the caller ID on his phone identified the caller was contacting him from St. Charles Medical Center.

Additional BMC patients reported being told by CHC/CCC via phone calls and/or in person that BMC was no longer offering chemotherapy treatment, that BMC was closing its Oncology practice and that they should transfer their care to CCC. One former CCC patient notified BMC that she questioned CCC staff about how they knew of her husband's new diagnosis upon first appointment at CCC without CCC being told in advance. The CCC staff person responded, "we have our ways." BMC staff became aware of additional similar reports.

BMC launched an investigation February 20, 2009. This included a review of EMR access during the period of the on-call arrangement with CCC. It was discovered that during the period of time between entering into an agreement with CCC to assist with on-call oncology coverage and the date of the investigation, 831 patient records were accessed over 3,300 times. It was estimated that only between five and ten patients had accessed after hours on-call service during that period of time whom may have required access to BMC's EMR.

Access to BMC's EMR by CCC workforce members with access to BMC's EMR for the agreed upon on-call coverage service was terminated February 27, 2009 following the investigation and at the time the on-call agreement was terminated. CCC VP Medical Staff Affairs Dr. Alan Ertle was notified of the breach. BMC terminated CCC workforce access for affected workforce members.

Following termination of access, BMC was notified by a patient on March 6, 2009 that the patient was contacted by CCC and informed that she "had" to receive treatment at CCC. Given this followed termination of access to

BMC's EMR, it appears that contact with this patient was for the purpose of marketing and providing the patient misinformation regarding her treatment. This falls under the category of marketing that is specifically prohibited by BMC policy and by the HIPAA Privacy Rule (45 CFR 164.508(a)(3)) without specific authorization from the patient.

Marvin Lein, BMC CEO notified CHC's president/CEO, Jim Diegel, February 27, 2009 of the results of BMC's preliminary investigation and what appeared to be inappropriate access to BMC's EMR by CHC CCC workforce members during a face-to-face meeting. Subsequent to the meeting Mr. Lein documented the conversation in a letter to Mr. Diegel dated March 1, 2009. BMC further indicated this appeared to be a violation of the HIPAA privacy rule and was interested in participating with CHC in a joint investigation of the incident. Post the face-to-face meeting, CHC declined at least four BMC requests for meetings to address the issue and resolve it in a cooperative manner. CHC legal counsel threatened to take legal action against BMC for "defamation" should the issue be made known by BMC to affected patients.

Through counsel, CHC proposed to jointly use an external expert to investigate. BMC declined the offer as BMC believed it was required to perform an investigation to determine the extent of any breach of its patient records that the results of its investigation must be made known to patients whose records were improperly accessed. CHC was not in agreement with that belief. CHC reissued its threat to take legal action against BMC should patients be notified of the event.

On March 3, 2009 and subsequently on March 19, 2009 CHC asserted that its preliminary investigation indicated no HIPAA violations had occurred because access was for "treatment, payment and healthcare operations" and all access was appropriate.

CHC refused to acknowledge the written on-call agreement and the established restrictions related to access to BMC's EMR and the BMC executed business associate contracts. In this instance, CCC was not acting as a covered entity but as a business associate and therefore was required to adhere to the requirements of BMC's on-call agreement and business associate contract

	<p>which did not allow blanket access to BMC's EMR.</p> <p>Pursuant to the Oregon Identity Theft Protection Act (ORS 646A.604(1)) a subset of patients (Category 1) were notified of the breach given the social security number was present in the records inappropriately accessed. Such notification was required by Oregon law. Notification was mailed to the patients March 27, 2009. This subset included patients where it was highly probable access was for purposes other than patient care or afterhours care coverage for BMC.</p> <p>CHC was provided a list of remaining patient files accessed and the frequency of access by BMC on March 27, 2009 to provide CHC the necessary data to further investigate potential inappropriate access by CCC workforce members. CHC was required to respond specifically to each unauthorized access and document that access was appropriate within ten days from the date of BMC counsel's letter to allow for prompt breach notification pursuant to ORS 646A.604(1) if access was not in accordance with the contractual arrangement between BMC and CHC related to on-call oncology coverage and executed business associate contracts.</p> <p>As of the date of this report, no specific accounting has been received from CHC. In addition, given CHC CCC was acting as a business associate of BMC, it is BMC's position that any access outside of access for on-call support purposes would represent a violation of the existing agreement and BMC business associate contract even if access were for other purposes related to CCC's treatment, payment and healthcare operations.</p> <p>On May 26, CHC acknowledged the existence of the on-call agreement's strict use limitations but stated such was never communicated to CCC providers and staff. In fact, the Agreement containing the on-call only limitation was specifically copied to both CHC VP Medical Affairs Dr. Alan Ertle and CCC Oncology Medical Director Dr. Steven Kornfeld by the then EVP Joe Smith, who created and approved of the Agreement on behalf of CHC. (see Exhibit A) CHC continues to deny physician and staff knowledge of the Agreement.</p>
<p>2. What data elements were involved and the extent of the data involved in the breach.</p>	<p><u>Data Elements:</u></p> <ul style="list-style-type: none"> • Patient full medical record (read only)

	<ul style="list-style-type: none"> • Patient scheduling <p><u>Extent of Data:</u></p> <p>It appears that BMC patient data and related appointment scheduling data was accessed for purposes other than the call coverage Agreement, which was inappropriate. It may also have involved creating of a paper record of patient information by CCC using screen prints or manual recording of patient information including appointment scheduling.</p>
<p>3. Description of the unauthorized person known or reasonably believed to have improperly used or disclosed PHI.</p>	<p>It has been documented that the following CCC workforce members may have accessed BMC's EMR for purposes other than on-call coverage for BMC oncology patients:</p> <ul style="list-style-type: none"> • Robert Boone, MD • Gina James • Lisa Jensen • Steven Kornfeld, MD • William Martin, MD • Angela Swanson
<p>4. Description of where the PHI is believed to have been improperly transmitted, sent or utilized.</p>	<p>PHI was accessed by the above listed CCC workforce members using assigned credentials that authorized access to BMC's EMR for the purpose of oncology on-call coverage. Such access did not permit the identified individuals to generally access BMC patient records for "treatment, payment or healthcare operations."</p>
<p>C. Apparent purpose(s) of access.</p>	<p>At least in part, intent to solicit or market CCC services to BMC patients and cause patients to change treatment providers.</p>
<p>D. Impact of Incident -potential misuse of data, identity theft, etc.</p>	<p>It does not appear PHI was inappropriately disclosed beyond CHC CCC workforce members. No documentation or related proof is available, however, to indicate further use and disclosure did not occur. Based on BMC patient complaints, it appears BMC patient data was used, at least in part, to encourage patients' to change care from BMC to CCC and to misinform patients regarding where treatment was to be provided (CCC versus BMC).</p>
<p>E. Whether any federal or state laws requiring individual notifications of breaches are triggered.</p>	<p>PHI was disclosed and the data disclosed included the patients' names and social security number. Unless it can be determined that access was appropriate and in accordance with the BMC on-call agreement and BMC business associate contract, Oregon law requires notification of all patients where patient records were</p>

	inappropriately accessed because social security numbers were disclosed along with the patient name.
F. Mitigation - steps to reduce any harmful effects known to the covered entity as a result of the unauthorized use or disclosure of PHI.	<p>CCC workforce member access was terminated February 27, 2009 at the same time the on-call relationship between BMC and CCC was terminated. BMC made attempts to work with CHC to investigate the unauthorized access and take the necessary steps to mitigate any damage. CHC CEO Jim Diegel met with BMC CEO on February 27th but declined to accept BMC CEO's Marvin Lein's further meeting requests as the investigation moved forward. CHC Board Chair Mr. Todd Taylor also declined a meeting request.</p> <p>BMC notified 34 patients of the breach and included the appropriate language to assist patients address prevention of potential identity theft as required by Oregon law. The patients notified were notified because it was determined that access to their medical records was highly likely not for patient care or for purposes of fulfilling CCC's agreed upon on-call staffing support.</p> <p>The notification of an additional approximately 800 BMC patients whose records were viewed by CCC without purpose under the on-call Agreement will occur on or before the week of June 14th. Patients will be provided information on how to request a full audit report of the medical record and what rights they have to file a HIPAA complaint with CHC and or the Office of Civil Rights.</p>
G. Corrective Action - steps to prevent reoccurrence.	See recommendations.
H. Additional information – such as notification to other facility's units or Fraud Prevention and/or police, licensing boards, etc.	<p>Pursuant to information available from the Department of Consumer and Business Services, the Bend Police Department was notified of the breach on April 3, 2009 and assigned a case number. A detective interviewed BMC representatives on April 8, 2009. BMC notified Bend Police on April 9th that it had no reason to believe criminal activity was involved but was filing for purposes of complying with Oregon identity theft law.</p> <p>On or about June 4th, the DA's office determined no cause for criminal charges, indicating patient social security and other protected information was not used for identity theft. The DA's determination was consistent with BMC's letter of April 9th in which BMC notified law enforcement it did not consider the situation to be criminal but was filing in order to comply with Oregon law.</p>



	<p>BMC will notify patients and post the results of the independent expert investigation to ensure patients have access to the facts and are afforded the ability to pursue their own informed actions. CHC reissued its threat to take legal action should BMC notify affected patients of the unauthorized viewing of their medical records.</p> <p>BMC revised its policy of providing access to external care givers to ensure frequent audits to prevent others from inappropriately accessing protected healthcare information (PHI).</p>
--	---



Exhibit A

From: Joseph Smith [mailto:jnsmith@cascadehealthcare.org]
Sent: Wednesday, December 24, 2008 12:54 PM
To: Randal Avolio
Subject: RE: Call Coverage Agreement- Medical Oncology

Thanks Randal, we will proceed accordingly. Joe

From: Randal Avolio [mailto:RAvolio@BMCTOTALCARE.COM]
Sent: Wednesday, December 24, 2008 12:48 PM
To: Joseph Smith
Cc: Marvin Lein; Lesley Camire; Melanie Brown; Dr. Rogers
Subject: RE: Call Coverage Agreement- Medical Oncology

Agreed.

Thank you.

Randal E. Avolio
Chief Operating Officer
Bend Memorial Clinic, PC.
1501 NE Medical Center Drive
Bend, Oregon 97701
541-460-3757 (direct)
ravolio@bmctotalcare.com
www.bendmemorialclinic.com

Bend Memorial Clinic - 80 physicians. 30 specialties. 60 years. We call it total care. You call it life.

From: Joseph Smith [mailto:jnsmith@cascadehealthcare.org]
Sent: Wednesday, December 24, 2008 12:04 PM
To: Randal Avolio
Cc: Alan Ertle; Stephen Kornfeld
Subject: RE: Call Coverage Agreement- Medical Oncology
Importance: High

Hello Randal, I have had extensive conversations with the appropriate people on this end and the following is what we believe will work for all concerned.

- Effective today, Cancer Care of the Cascades physicians will include Br. Braich in their call coverage rotation. As of today, Dr. Braich's call frequency will be one in four. In February, with the addition of a fourth medical oncologist into CCoC, the call frequency for Dr. Braich will go to one in five. The schedule for call will be established between the providers themselves.
- This arrangement will remain in place until such a time as BMC adds a second medical oncologist (Locums or permanent). Upon the first day of practice for BMC's second medical oncologist, the call coverage agreement is canceled. Once canceled, the call coverage agreement will not be re-instated even if BMC's second medical oncologist (Locums or permanent) subsequently leaves or does not have their contract with BMC renewed,



- As part of the agreement the following will be included:
 1. BMC will provide at no cost to CCoC, view only access to the medical records for patients treated as part of this coverage agreement. This access will be provided to those individuals (physicians and appropriate support staff) named by CCoC and authorized by BMC. Access to the medical records is subject to all applicable regulations.
 2. CCoC will bill and collect for services provided to BMC patients treated under this agreement.
 3. BMC will bill and collect for services provided by Dr. Braich under this agreement.

Randal, it is my intention to execute the appropriate formal agreement in the very near future. Until that time, this communication shall serve as our complete and binding agreement. To put this into effect, please respond in the affirmative with a return e-mail today if possible. Please be aware that the current call coverage arrangement, which I believe to be informal, expires at the end of December and will not be renewed. This e-mail agreement, when approved by BMC, replaces the existing agreement.

Thanks for your help in reaching a resolution to this issue. Please call me at 541-706-5819 if you have questions. You can also call my cell at 701-238-9603. Thanks and Happy Holidays. Joe