Buchanan Ingersoll & Rooney PC
Attorneys & Government Relations Professionals

One Oxford Centre
301 Grant Street, 20th Floor
Pittsburgh, PA 15219-1410
T 412 562 8800
F 412 562 1041
www.buchananingersoll.com

Pamela E. Hepp
412 562 1418
pamela.hepp@bipc.com

November 22, 2013

VIA FAX - 603-271-2110

Attorney General Joseph Foster
New Hampshire Department of Justice
33 Capitol Street
Concord, New Hampshire 03301

Re: DATA SECURITY INCIDENT

Dear Mr. Foster:

I am writing to you on behalf of my client Genesis Rehabilitation Services ("GRS"), a Pennsylvania corporation that provides rehabilitation therapy and wellness services across the nation. GRS learned on or about September 3, 2013 that two USB drives, which a GRS employee left in her office, were missing. These USB drives contained the protected health information of 739 Lebanon Center and Wheelock Terrace patients and the personal information of 25 GRS employees, agency employees, or applicants who are also residents of New Hampshire.

GRS has no information indicating that the personal information contained on the thumb drives was inappropriately used or accessed by or redisclosed to anyone. However, out of an abundance of caution, GRS is providing notice pursuant to N.H. Rev. Stat. § 359-C:20 of a data security incident to the Attorney General and the persons whose data was included on the lost USB drives.

What Happened

On or about September 3, 2013, GRS discovered that two USB drives, which were left in an office, went missing on August 30, 2013. These USB drives contained emails and attachments that documented protected health information and personal information relating to certain Lebanon Center and Wheelock Terrace facility patients and GRS employees, agency employees, or applicants.

The protected health information of the patients stored on the USB drives may have included patient name, date of birth, date of admission or service, age, gender, facility name, attending nurse or physician name, medical record number, diagnosis, injury, and treatment. In

addition, of the 739 patients, the social security numbers of 71 patients were included on the USB drive. The remaining 668 patients' social security numbers were not included on the USB drive. For the affected employees, agency employees or applicants, the information stored on the USB drives may have included name, address or email address, and social security number.

Upon discovering this loss, GRS immediately initiated an extensive search to locate the missing USB drives. Furthermore, once GRS learned that the USB drives were missing, GRS reported the incident to law enforcement and continues to cooperate with its investigation.

What GRS is Doing About It

This is a serious matter, and GRS has taken steps to address it and prevent any further unauthorized use or disclosure of its employee's personal information and the protected health information of the individuals it serves, including the following:

- Immediately counseled the employee who lost the drives on the importance of following GRS policy that states that only encrypted USB travel drives may be utilized;
- Continuing to encrypt and protect employee and patient data through secure SSL technology;
- Updating our company policies and procedures on data security and privacy; and
- Enhancing company-wide data security awareness of the importance of data security and patient and employee privacy.

Additionally, GRS is providing one year of free credit monitoring, should the individual wish to activate the service. GRS is also offering an insurance reimbursement component of up to $25,000 for reasonable and necessary expenses incurred as a result of becoming a victim of identity theft.

Based on what GRS has learned, GRS began notifying the 35 employees via U.S. Mail starting on October 22, 2013. During that time, GRS continued investigating the breach in terms of the 739 patients and began sending letters to the affected patients via U.S. Mail starting on November 7, 2013. Copies of the notices sent to the residents are attached hereto.

Please do not hesitate to contact me at 412 562 1418 if you have questions or concerns.

Very truly yours,

Pamela E. Hepp

Pamela E. Hepp

Enclosure

October 24, 2013

[redacted]

Dear [redacted],

We are writing to inform you that on or about September 3, 2013, the Genesis Rehabilitation Services (GRS) staff providing services at Lebanon Center discovered that there may have been unauthorized access to certain of your personal information as an employee, agency employee or applicant of GRS. Specifically, as part of our investigation, we discovered that a GRS employee's USB drive that had been left in a secure office in the center was missing.

This USB drive contained the names, addresses or email addresses and social security numbers of thirty-three employees, agency employees or applicants of GRS. GRS has no information indicating that the personal information contained on the USB drive was inappropriately used by, accessed by, or re-disclosed to anyone. However, out of an abundance of caution, GRS is providing notice of a data security incident to those individuals whose data we believe may have been present on the lost USB drive.

Upon discovering this loss, GRS immediately initiated an extensive search at Lebanon Center to locate the missing USB drive. Furthermore, once we learned that the USB drive was missing, we reported the incident to law enforcement and continue to cooperate with their investigation. Since then, we have taken the following steps to ensure that something like this does not happen again:

- Immediately counseled the employee who lost the drive on the importance of following GRS policy that states that only encrypted USB travel drives may be utilized;
- Continuing to encrypt and protect employee and resident data through secure SSL technology;
- Updating our company policies and procedures on data security and privacy; and
- Enhancing company-wide data security awareness of the importance of data security and patient and employee privacy.

We are notifying you of the incident because your information, including your social security number, may have been contained on the USB drive. Although we have no information

indicating that the personal information was inappropriately used or accessed, we are notifying you so that you may take steps to protect yourself.

We encourage you to remain vigilant and to contact us in the event you learn of any unauthorized use of your personal information. In light of the potential loss of protected personal information, GRS in an abundance of caution would like to provide you one year of free credit monitoring and resolution services to insure protection against any identity theft as a result of this incident. We have contracted with Kroll to extend this service to you. The services will include:

- Free credit monitoring for 12 months.
- An insurance reimbursement component of up to $25,000 for reasonable and necessary expenses incurred as a result of becoming a victim of identity theft.

If you would like to take advantage of these services, please contact the office of the Genesis Compliance Officer, Harry Alberts. The Compliance Department will provide you with the necessary information you will need to initiate this service with Kroll. The Genesis Compliance Department can be reached at 1-800-944-7776.

We recommend that you remain vigilant by regularly reviewing your credit reports and account statements for any unauthorized activity. If you do find suspicious activity on your credit reports or become aware of identity theft, we recommend that you call your local law enforcement office, file a police report of identity theft, and obtain a copy of the police report, as you may need to give copies of the police report to creditors to clear up your records.

We take our responsibility to protect your personal information very seriously and have taken appropriate steps to help prevent something like this from ever happening again. If you have any further questions, please contact Harry Alberts, the Genesis Compliance Officer, by phone at 1-800-944-7776. We apologize for any inconvenience caused to you as a result of these events and want to reassure you that maintaining the confidentiality of your data remains a priority to us.

Very truly yours,

Harry Alberts
Compliance Officer
Vice President Compliance and Internal Audit

Genesis Rehab Services®

<<Date>> (Format: Month Day, Year)

<<Lastname>>
<<Address1>>
<<Address2>>
<<City>>, <<Stateprovince>> <<Postalcode>>
<<Intelligent Mail Barcode>>

To the Family Member of <<Firstname>> <<Middlename>> <<Lastname>>,

Genesis Rehabilitation Services strives to abide by the requirements protecting the confidential health information of all its patients. This standard is part of our Standard of Conduct, and a duty which our employees, as health professionals, work diligently to keep. However, we are writing to inform you of an incident that may have exposed some of your loved one's personal healthcare information, and of services we are offering to your loved one to relieve concerns about the incident.

On or about August 30, 2013 a Universal Serial Bus (USB) data drive (sometimes referred to as a "thumb" drive) with information about former and current residents of Lebanon Center and Wheelock Terrace was lost by a therapy staff member at the Lebanon Center. This issue was discovered on September 3. Upon discovering the loss, the staff member initiated an extensive search to locate the missing USB drive. Furthermore, once we learned that the USB drive was missing, we reported the loss to local law enforcement authorities and continue to cooperate with their investigation.

We are notifying you of this incident because your loved one's information may have been contained on the USB data drive. Based on our review, the information on the USB may have included the name of the patient, date of birth,<<ClientDef2(social security number, medical insurance identification numbers,)>> information about treatment and diagnoses, and dates of service. No credit card data or other financial information was stored on the device. Although we have no indication that the information on the drive has been accessed, misused, or re-disclosed, we are notifying you so that you may take steps to protect your loved one.

We will continue to take the following steps to ensure that a similar situation does not happen again:

- Immediately counseled the staff member who lost the USB data drive on the importance of following company policy that states that only encrypted USB data drives may be utilized;
- Continuing to encrypt and protect employee and resident data through secure SSL technology;
- Updating our company policies and procedures on data security and privacy; and
- Enhancing company-wide data security awareness of the importance of data security of patient privacy.

We encourage you to remain vigilant and to contact us in the event you learn of any unauthorized use of your loved one's personal information. Although we have no indication that the information has been inappropriately access or used, out of an abundance of caution and because securing your loved one's personal information is so important to us, we have engaged Kroll Advisory Solutions to provide identity theft safeguards at no cost to your loved one for 1 year through its ID TheftSmart™ program. Your loved one's identity theft safeguards include Enhanced Identity Theft Consultation and Restoration. The enclosed materials describe these services and instructions on how to receive your services are listed in the *"Next Steps"* box on the second page of this letter.

If you have any questions, want more information about this incident, or feel that your loved one may have an identity theft issue, you may call the following toll-free telephone number: 1-877-451-9362, 8:00 a.m. to 5:00 p.m. (Central Time), Monday through Friday.

We deeply regret this incident and apologize for any inconvenience this may cause to you or your loved one. Maintaining the confidentiality of your information is and continues to be a priority for us. We trust that the quality and reliability of the support services being offered demonstrate our continued commitment to your loved one's security.

Sincerely,

Harry Alberts
Compliance and Privacy Officer

Next Steps

Your loved one's membership number is: <<MEMBERSHIPNUMBER>>

Call 1-877-451-9362 if you need help or have questions
8 a.m. to 5 p.m. (Central Time), Monday through Friday
Kroll representatives are ready to help you.