# North Carolina Security Breach Reporting Form
## Pursuant to the Identity Theft Protection Act of 2005

Name of Business Owning or Licensing Information Affected by the Breach: Pediatric Services of America, Inc.
Address: 310 Technology Parkway
Norcross, Georgia 30092
Telephone: (770) 840-3234
Fax: (770) 840-3234
Email: jhamilton@psahealthcare.com

**PLEASE SUBMIT FORM TO:**
Consumer Protection Division
NC Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
Telephone: (919) 716-6000
Toll Free in NC: (877) 566-7226
FAX: (919) 716-6050

Date Security Breach Reporting Form submitted: 8/15/06 (Original notice letter sent 8/7/06)

Date the Security Breach was discovered: 07/15/06

Estimated number of affected individuals: 51,000 nationwide

Estimated number of NC residents affected: 7,089

Name of business maintaining or possessing information that was the subject of the Security Breach, if the business that experienced the Security Breach is not the same entity as the business reporting the Security Breach (pursuant to N.C.G.S. § 75-65(b): N/A

Describe the circumstances surrounding the Security Breach and state whether the information breached was in electronic or paper format: Company-owned laptop computer was stolen from an employee's car on 7/15/06; computer contained sensitive personal data in an electronic format.

Regarding electronic information breached, state whether the information breached or potentially breached was password protected or encrypted in some manner. Yes If so, please describe the security measures protecting the information: The laptop computer was password protected. The data was not encrypted.

Describe any measures taken to prevent a similar Security Breach from occurring in the future: Policies & Procedures have been revised to limit and restrict downloading of sensitive personal data; we are deleting individual Social Security Numbers from our data systems; and, we intend to encrypt all sensitive personal information.

Date affected NC residents (were) will be notified: Notice letters sent on 8/8/06

If there has been any delay in notifying affected NC residents, describe the circumstances surrounding the delay pursuant to N.C.G.S. § 75-65(a) and (c)): N/A

**If the delay was pursuant to a request from law enforcement pursuant to N.C.G.S. § 75-65(c), please include the written request or the contemporaneous memorandum.**

How NC residents (were) will be notified? (pursuant to N.C.G.S. § 75-65(e))
**Please attach copy of the notice if in written form or a copy of any scripted notice if in telephonic form.**

- [x] written notice
- [ ] electronic notice (email)
- [ ] telephone notice
- [ ] substitute notice

Signature: John R. Hamilton III Date: 8/15/06
Contact Person, Title: John R. Hamilton III, General Counsel
Address: Same as above
(if different from above)
Telephone: (770) 840-3234 Fax: (770) 840-3234 Email: jhamilton@psahealthcare.com

**HealthCare**

August 8, 2006

[Guar-Name]
[Guar-Address1]
[Guar-Address2]
[Guar-City], [Guar-State] [Guar-Zip]

Re: Notice Regarding Potential Theft of Patient Information
**Control # [Control #]**

Dear [Guar-Name]:

We are writing to inform you that confidential patient information contained on a laptop computer of an employee of Pediatric Services of America ("PSA") may have been obtained by an unauthorized individual following the theft of the laptop computer from the PSA employee's car on July 15, 2006. We sincerely regret that this incident has occurred and apologize for any inconvenience that it causes you. To date, the laptop computer has not been recovered. Unfortunately, the records on the laptop computer appear to have contained confidential information about *[Patient]*, including some or all of the following: name and address, Social Security Number, and medical diagnostic and treatment information used in the preparation of reimbursement claims for services provided by PSA to *[Patient]*. It should be noted that the confidential information did not include any banking information or credit card numbers.

We would like to assure you that we are working diligently with law enforcement to identify and prosecute the responsible person(s) and to recover the stolen laptop computer. We have also initiated our own investigation and will continue our efforts to locate the laptop as well as take steps to enhance the security of our confidential patient records contained on other PSA computers. More importantly, we want you to be aware of the situation so that you can take precautions to protect yourself against the possibility of becoming a victim of identity theft from any unauthorized acquisition of your Social Security Number or other information.

In order to help minimize the possible future misuse of patient information, we suggest you immediately consider taking the steps outlined on the attached sheet entitled "IMPORTANT STEPS TO HELP PREVENT FRAUD," including calling the toll-free number referenced in item #7. The attached information page covers these points in more detail, and includes explanations as to how these actions can help protect *[Patient]* from becoming a potential victim of identity theft.

We stand ready and willing to provide you assistance. Again, we sincerely regret that this theft has occurred and we will be doing all that we can to protect the confidential patient information in our possession and minimize any further inconvenience to you.

Yours truly,

Daniel J. Kohl
President & Chief Executive Officer

## IMPORTANT STEPS TO HELP PREVENT FRAUD

1. **Carefully review all of your banking and credit card account statements issued since July 15, 2006 and report any unauthorized transactions to the applicable bank or credit card company**. You may wish to consider changing the account numbers on your existing banking and credit card accounts if you see any suspicious activity. This will help you to avoid future risk by eliminating the ability of unauthorized individuals to access your accounts through the use of your old account numbers.

2. **Notify your financial institution(s) and credit card companies that you received this notice.** This will provide them with notice that information relating to you may have been viewed or accessed by an unauthorized party.

3. **Contact the fraud department at the three major credit bureaus listed below and ask them to place a "fraud alert" on your credit file**. When you place an initial fraud alert with one of the bureaus, your request will be automatically forwarded to the other bureaus which, in turn. will also place fraud alerts on your credit file. ***Please note***: placing a fraud alert on your credit file will make it more difficult for a criminal to open a fraudulent account in your name; however, it may also make it more difficult for you to open a new account as well because extra steps in the approval process will be required to verify your identity. Although we recommend that you place a fraud alert on your credit file as a precautionary measure, you may wish to discuss with the credit bureau how you might minimize inconveniences to you during the time the fraud alert is active.

   **Experian:** **(888) 397-3742 or** www.experian.com
   **Equifax:** **(877) 478-7625 or** www.equifax.com
   **TransUnion:** **(800) 680-7289 or** www.transunion.com

4. **Obtain a copy of your credit report from each of the three major credit reporting agencies and review them to be sure they are accurate and include only authorized accounts.** You are entitled to one free copy of your report annually. To order your report, you may visit www.annualcreditrreport.com or call toll-free (877) 322-8228. Carefully review your credit report to verify that your name, address, account, and any other information is accurate and notify the credit reporting agencies of any errors you detect.

5. **Visit the Federal Trade Commission's ("FTC") website at www.ftc.gov to obtain additional information about how to protect against identity theft.** You may also wish to contact the FTC at (877) FTC-HELP (877-382-4357) or TTY: (866) 653-4261 if you have further general questions about identity theft.

6. **Remain vigilant over the next 12 to 24 months and report any suspected incidents of identity theft or other misuse of your personal information immediately.**

7. **You may call us toll-free immediately at 1-866-752-5259, as we have set up a 24-hour/7-day per week information service to document your questions or concerns about this matter.**