

23218

101 Munson Street, Suite 201  
Greenfield, MA 01301  
Info@LifePathMA.org  
www.LifePathMA.org



---

**Letter to consumer with SS number breach**

September 27, 2021

Dear [Member Name],

I'm writing to inform you of a privacy incident that took place where a LifePath employee may have shared your personal information for the purposes of having unauthorized individuals access secure databases to enter documentation related to evaluations. This letter provides information about the outcome of our investigation into this incident and steps you can take if you are concerned about the potential misuse of your personal information.

**Our Investigation and Response**

On January 29, 2021, LifePath was made aware of the incident through an U.S. Department of Health and Human Services, Office for Civil Rights complaint. The complaint alleged the employee shared login credentials with other individuals for the purpose of completing clinical evaluations beginning in April 2020. The sharing of credentials was not authorized. Upon learning of this situation, LifePath immediately revoked the employee's user capabilities and access to electronic information and began its investigation, and their employment with the agency was terminated as of February 1, 2021. Please note that LifePath was required by law to delay sending this notice as a result of a law enforcement referral.

LifePath conducted an investigation, which included a review of the employee's volume of work, access to personal health information, and evidence provided by the complaint. Our investigation found that there is sufficient evidence to indicate that this person may have shared login credentials as well as your name, date of birth, address, phone number, Social Security Number, and clinical information. Health information, inclusive of medications, medical conditions, assessments, and physicians could have been accessed by an unauthorized individual.

LifePath takes privacy seriously. Our staff are well trained and held to all applicable legal standards, and our data is secure. This was the unauthorized action of an individual, despite signed confidentiality agreements. In response to this incident, LifePath has strengthened its tracking measures, is increasing log audits, and will continue to take additional steps to limit how much personal information can be seen and by whom.

**What You Can Do**

Our investigation has given us no reason to believe that your information has been further used in an impermissible manner. Nevertheless, there are some things you can do if you are concerned about the potential misuse of your personal information.

You may contact one or more of the three major consumer reporting agencies to take the following steps:



Phone: 413-773-5555 | 978-544-2259  
Toll free: 800-732-4636 | Fax: 413-772-1084



**LifePath**  
options for independence

101 Munson Street, Suite 201  
Greenfield, MA 01301  
Info@LifePathMA.org  
www.LifePathMA.org

---

**Letter to consumer without SS number breach**

September 27, 2021

Dear [Member Name],

I'm writing to inform you of a privacy incident that took place where a LifePath Employee may have shared your personal information for the purposes of having unauthorized individuals access secure databases to enter documentation related to evaluations. This letter provides information about the outcome of our investigation into this incident and steps you can take if you are concerned about the potential misuse of your personal information.

**Our Investigation and Response**

On January 29, 2021, LifePath was made aware of the incident through an U.S. Department of Health and Human Services, Office for Civil Rights complaint. The complaint alleged the employee shared login credentials with other individuals for the purpose of completing clinical evaluations beginning in April 2020. The sharing of credentials was not authorized. Upon learning of this situation, LifePath immediately revoked the employee's user capabilities and access to electronic information and began its investigation, and their employment with the agency was terminated as of February 1, 2021.

LifePath conducted an investigation which included a review of the employee's volume of work, access to personal health information, and evidence provided by the complaint. Our investigation found that there is sufficient evidence to indicate that this person may have shared login credentials as well as your name, date of birth, address, phone number and clinical information. Health information, inclusive of medications, medical conditions, assessments, and physicians could have been accessed by an unauthorized individual.

LifePath takes privacy seriously. Our staff are well trained and held to all applicable legal standards, and our data is secure. This was the unauthorized action of an individual, despite signed confidentiality agreements. In response to this incident, LifePath has strengthened its tracking measures, is increasing log audits, and will continue to take additional steps to limit how much personal information can be seen and by whom.

**What You Can Do**

Our investigation has given us no reason to believe that your information has been further used in an impermissible manner. Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. However, to our knowledge there has not been a report filed. Nevertheless, there are some things you can do if you are concerned about the potential misuse of your information.



Phone: 413-773-5555 | 978-544-2259  
Toll free: 800-732-4636 | Fax: 413-772-1084

You may contact one or more of the three major consumer reporting agencies to take the following steps:


- Notify them of the loss of your personal information and request an initial fraud alert to be placed on your credit for 90 days.
- Order a credit report and review it for any signs of fraud on any accounts. For example, look for inquiries listed on the credit report from businesses that accessed your credit without your request.
- Request a security freeze which will restrict the opening of new accounts using your information. *There is no charge to request a security freeze.* Please note that requesting a security freeze on your credit may delay, interfere with or prevent timely approval of any requests made by you for new loans, credits, employment, housing or other services.

Additional information concerning contact information for consumer reporting agencies and instructions on how to request a security freeze are enclosed with this letter.

We are sorry that this incident has occurred. LifePath takes the confidentiality of your personal information very seriously, and we regret any inconvenience or concern this incident has caused you. If you have any questions, please contact our dedicated data breach staff at **1.833.678.2100**.

Sincerely,

Barbara Bodzin



Executive Director



**LifePath**  
options for independence

101 Munson Street, Suite 201  
Greenfield, MA 01301  
Info@LifePathMA.org  
www.LifePathMA.org

---

**Letter to surrogate of consumer with SS number breach**

September 27, 2021

To whom it may concern,

I'm writing to inform you of a privacy incident that could have affected the PCA consumer you provide surrogate services for via LifePath, Inc. This letter provides information about the outcome of LifePath's investigation into this incident and steps to be taken if the consumer is concerned about the potential misuse of their personal information.

**Our Investigation and Response**

On January 29, 2021, LifePath was made aware of the incident through an U.S. Department of Health and Human Services, Office for Civil Rights complaint. The complaint alleged an employee shared login credentials with other individuals for the purpose of entering data into clinical evaluations beginning in April 2020. The sharing of credentials was not authorized. Upon learning of this situation, LifePath immediately revoked the employee's user capabilities and access to electronic information and began an investigation. Employment with the agency was terminated as of February 1, 2021. Please note that LifePath was required by law to delay sending this notice as a result of a law enforcement referral.

LifePath's investigation included a review of the employee's volume of work, access to personal health information, and evidence as provided by the complainant. We found that there is sufficient reason to believe this person may have shared login credentials as well as the consumer's name, date of birth, address, phone number, Social Security Number, and health information; inclusive of medications, medical conditions, assessments, and physician information.

LifePath takes privacy seriously. Our staff are well trained and held to all applicable legal standards, and our data is secure. This was the unauthorized action of an individual, despite signed confidentiality agreements. In response to this incident, LifePath has strengthened its tracking measures, is increasing log audits, and will continue to take additional steps to limit how much personal information can be seen and by whom.

**What You Can Do**

Our investigation has given us no reason to believe that the consumer's information has been further used in an impermissible manner. Nevertheless, there are some things to be done if you are concerned about the potential misuse of their personal information.

One or more of the three major consumer reporting agencies can be contacted to take the following steps:



Phone: 413-773-5555 | 978-544-2259  
Toll free: 800-732-4636 | Fax: 413-772-1084

- Notify them of the loss of the consumer's personal information and request an initial fraud alert to be placed on their credit for 90 days.
- Order a credit report and review it for any signs of fraud on any accounts. For example, look for inquiries listed on the credit report from businesses that accessed their credit without a request.
- Request a security freeze which will restrict the opening of new accounts using their information. *There is no charge to request a security freeze.* Please note that requesting a security freeze on someone's credit may delay, interfere with or prevent timely approval of any requests made by them for new loans, credits, employment, housing or other services.

Additional information concerning contact information for consumer reporting agencies and instructions on how to request a security freeze are enclosed with this letter.

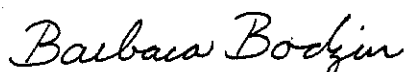
If you are concerned about the potential misuse of the consumer's personal information we would like to offer them 18 months of credit monitoring to lower any risk of identity theft. Please call **1.833.678.2100** to request credit monitoring.

Under Massachusetts law, your consumer has the right to obtain any police report filed in regard to this incident. However, to our knowledge there has not been a report filed.

We are sorry that this incident has occurred. LifePath takes the confidentiality of personal information very seriously, and we regret any inconvenience or concern this incident has caused you and your consumer. If you have any questions, please contact our dedicated data breach staff at **1.833.678.2100**.

Sincerely,

Barbara Bodzin



Executive Director



---

**Letter to surrogate of consumer without SS number breach**

September 27, 2021

To whom it may concern,

I'm writing to inform you of a privacy incident that could have affected the PCA consumer you provide surrogate services for via LifePath, Inc. This letter provides information about the outcome of LifePath's investigation into this incident and steps to be taken if the consumer is concerned about the potential misuse of their personal information.

**Our Investigation and Response**

On January 29, 2021, LifePath was made aware of the incident through an U.S. Department of Health and Human Services, Office for Civil Rights complaint. The complaint alleged an employee shared login credentials with other individuals for the purpose of entering data into clinical evaluations beginning in April 2020. The sharing of credentials was not authorized. Upon learning of this situation, LifePath immediately revoked the employee's user capabilities and access to electronic information and began an investigation. Employment with the agency was terminated as of February 1, 2021. Please note that LifePath was required by law to delay sending this notice as a result of a law enforcement referral.

LifePath's investigation included a review of the employee's volume of work, access to personal health information, and evidence as provided by the complainant. We found that there is sufficient reason to believe this person may have shared login credentials as well as the consumer's name, date of birth, address, phone number, and clinical information; inclusive of medications, medical conditions, assessments, and physician information. Health information, inclusive of medications, medical conditions, assessments, physicians could have been accessed by an unauthorized individual.

LifePath takes privacy seriously. Our staff are well trained and held to all applicable legal standards, and our data is secure. This was the unauthorized action of an individual, despite signed confidentiality agreements. In response to this incident, LifePath has strengthened its tracking measures, is increasing log audits, and will continue to take additional steps to limit how much personal information can be seen and by whom.

**What You Can Do**

Our investigation has given us no reason to believe that the consumer's information has been further used in an impermissible manner. Nevertheless, there are some things to be done if you are concerned about the potential misuse of their personal information.

One or more of the three major consumer reporting agencies can be contacted to take the following steps:



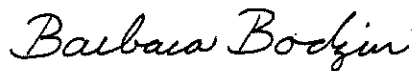
- Notify them of the loss of the consumer's personal information and request an initial fraud alert to be placed on their credit for 90 days.
- Order a credit report and review it for any signs of fraud on any accounts. For example, look for inquiries listed on the credit report from businesses that accessed their credit without a request.
- Request a security freeze which will restrict the opening of new accounts using their information. *There is no charge to request a security freeze.* Please note that requesting a security freeze on someone's credit may delay, interfere with or prevent timely approval of any requests made by them for new loans, credits, employment, housing or other services.

Additional information concerning contact information for consumer reporting agencies and instructions on how to request a security freeze are enclosed with this letter.

We are sorry that this incident has occurred. LifePath takes the confidentiality of personal information very seriously, and we regret any inconvenience or concern this incident has caused you and your consumer. If you have any questions, please contact our dedicated data breach staff at **1.833.678.2100**.

Sincerely,

Barbara Bodzin



Executive Director



---

**Credit Freeze instructions included in all mailings**

**How Can I Place a Free Credit Freeze?**

Experian.com, TransUnion.com and Equifax.com maintain dedicated web pages where you can set up credit freezes. When requesting a credit freeze online, the bureau may supply, or have you create, a personal identification number (PIN) or password to use when thawing or reactivating your freeze.

**Experian credit report**

To freeze your Experian credit report go to Experian.com, or you can write to Experian Security Freeze, P.O. Box 9554, Allen, TX 75013.

Written requests should include the following:

- Your full name including middle initial (and generation)
- Social Security number
- Complete addresses for the past two years
- Date of birth
- One copy of a government issued identification card, such as a driver's license, state ID card, etc.
- One copy of a utility bill, bank or insurance statement, etc.

Make sure that each copy is legible and displays your name and current mailing address and the date of issue. Send copies of any documents you wish to provide to us and always retain your original documents.

**Equifax credit report**

To place a security freeze on your Equifax credit report, go to Equifax.com to create a myEquifax account. You can view the status of your security freeze, and also temporarily lift or permanently remove the freeze through myEquifax. You can also call our automated line at (800) 349-9960 or call Customer Care at (888) 298-0045.

**TransUnion credit report**

To freeze your TransUnion credit report go to TransUnion.com or send a letter requesting a freeze and include the following information: Your name. Current address (If you have lived here less than 2 years, provide your previous address also) Your TransUnion file number (if applicable) Social Security number. Date of birth. Mail to: TransUnion P.O. Box 160, Woodlyn, PA 19094.





Consumers may also initiate a freeze by calling 888-909-8872. You can complete the process using an automated system or opt to speak with an agent.

### **How Can I Lift a Credit Freeze?**

The same web pages used to set up credit freezes can be used to remove or suspend them. All three bureaus also provide instructions for lifting a freeze by phone, using the password or PIN connected to your freeze at each bureau.

In addition to your ability to permanently unfreeze your credit, you may have the option to lift the freeze temporarily, either by granting one-time access to a specific creditor, or by indicating a length of time (one day, one week, etc.) you want the freeze to be suspended. Policies vary by bureau so make sure you understand what your options are before you begin the process.

When you enter your password or PIN online or by phone, your credit will be thawed within one hour. If you lose your password or PIN, the credit bureaus will need to verify your identity, which will delay the process.