**Table of Contents**

Executive Summary ............................................................................................................ 3

A. Summary of PIA Findings ............................................................................................. 4
B. Purpose of a PIA ........................................................................................................... 4
C. **Company X**<PIA scope> Description ..................................................................... 4
D. GAPP Alignment .......................................................................................................... 4
E. PCI DSS Compliance <Include section only if applicable> ............................................ 5
F. HIPAA Compliance <Include section only if applicable> ............................................. 6
G. <Put regulation/standard/etc. as applicable> <Include section only if applicable> ........... 6

Work Papers .......................................................................................................................... 7

1. Project Scope .................................................................................................................. 8
2. **Company X**<PIA scope> process ............................................................................. 9
3. Privacy Complaints and Incidents ................................................................................. 9
   4.1 Website Privacy Policies ............................................................................................ 10
   4.2 Internal Information Security and Privacy Policies ................................................. 10
5. Privacy Programs and Executive Support ..................................................................... 11
6. Awareness and Training ............................................................................................... 11
7. PII Collection and Access ............................................................................................ 11
   7.1 Customer PII Collection ........................................................................................... 11
   7.2 Use Limitation & Sharing Customer PII With Third Parties ...................................... 12
   7.3 Purpose Specification ............................................................................................... 12
   7.4 Individual Participation ............................................................................................ 13
8. Customer PII Storage ..................................................................................................... 13
10. Contractual Obligations ............................................................................................... 14
11. Background checks ..................................................................................................... 14
12. Safeguards & Data Integrity ....................................................................................... 15
13. Data Quality ................................................................................................................ 15
14. Customer PII Used for Test Purposes ......................................................................... 15
15. Limiting access within applications and systems ...................................................... 16
16. Oversight, Maintenance & Evaluation ........................................................................ 16
   16.1 Accountability .......................................................................................................... 16
   16.2 Openness ............................................................................................................... 17
   16.3 Customer PII Retention ........................................................................................... 17
   16.4 Customer PII Disposal ............................................................................................ 18
   16.5 Compliance and enforcement ................................................................................. 18

Appendix A – **Company X** Privacy Survey Responses ................................................... 19
Appendix B – Existing **Company X** Information Security and Privacy Policies ............... 20
Appendix C – Recommended Information Security and Privacy Policies & Supporting
Documents ............................................................................................................................ 21
Appendix D – **Company X** PIA Project Meeting Notes .................................................. 22
Appendix E – U.S. State Breach Notice Laws ................................................................... 23
Appendix F – **Company X** Website Privacy Policies ..................................................... 24
Appendix G - Data Protection (Privacy) Laws .................................................................... 25
Appendix H - **Company X** Information Security and Privacy Training and Awareness
Program ............................................................................................................................... 26
Appendix I - Recommended **Company X** Website Privacy Policy ................................ 27
Appendix J - Updated **Company X** Website Privacy Policy ........................................ 28
Appendix K – <Change to PIA Specific Issue> ................................................................. 29
Appendix L – <Change to PIA Specific Issue> ................................................................. 30
Appendix M – Updated **Company X** Security Policies ................................................. 31

Company X Privacy Impact Assessment  CONFIDENTIAL: For internal use only
© Rebecca Herold. All rights reserved.
# Executive Summary

<Intro/background>

| 1. Company information security and privacy administration | Findings summary |
| 2. Corporate leadership | Findings summary |
| 3. Data collection and processing | Findings summary |
| 4. Data retention | Findings summary |
| 5. Openness and transparency | Findings summary |
| 6. Responsiveness | Findings summary |
| 7. Hardware and software physical security | Findings summary |
| 8. Customer control | Findings summary |
| 9. Consent and opt-in/opt-out controls | Findings summary |
| 10. Privacy Enhancing Practices & Technology | Findings summary |
| 11. Privacy Invading Practices & Technology | Findings summary |

## Assessment & Justification

**LEGEND:**
- Green: Privacy-friendly and privacy enhancing
- Blue: Generally privacy aware but could be improved upon
- Yellow: Generally aware of privacy issues and requirements, but notable lapses exist
- Red: Substantial and comprehensive privacy threats
- Black: Significant lack of security for PII

Table 1 – <Company X>PIA summary
<Company X> PIA Report

A. Summary of PIA Findings

B. Purpose of a PIA

C. <Company X><PIA scope> Description

<table>
<thead>
<tr>
<th>Data Item</th>
<th>Data Item Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td></td>
</tr>
<tr>
<td>9.</td>
<td></td>
</tr>
<tr>
<td>10.</td>
<td></td>
</tr>
<tr>
<td>11.</td>
<td></td>
</tr>
<tr>
<td>12.</td>
<td></td>
</tr>
<tr>
<td>13.</td>
<td></td>
</tr>
</tbody>
</table>

Table 2 – Data Within <Company X><PIA scope> Processing

D. GAPP Alignment

1. Management, Accountability & Training

   <Put findings here>

Information Security and Privacy Training and Awareness Practices

   <Put findings here>

2. Notice & Purpose for PII Use
<Put findings here>

3. Choice & Consent to use PII

<Put findings here>

4. Collection of PII

<Put findings here>

5. Use and Retention of PII

<Put findings here>

6. Individual access

<Put findings here>

7. Disclosure and Limiting Use of PII

<Put findings here>

8. Security and Safeguards

<Put findings here>

9. Accuracy & Quality of PII

<Put findings here>

10. Openness, Monitoring & Challenging Compliance

<Put findings here>

E. PCI DSS Compliance <Include section only if applicable>

<Put findings here>
F. HIPAA/HITECH Compliance <Include section only if applicable>

<Put findings here>

G. <Put regulation/standard/etc. as applicable > <Include section only if applicable>

<Put findings here>
Work Papers

<Background info>

The recommendations include:

<Put recommendations here>

NOTE: This report is not, and should not be construed as, a legal opinion.
1. Project Scope

<Description>
2. **<Company X><PIA scope>** process

Figure 1 shows the **<Company X><PIA scope>** process.

*Figure 1 – <Company X><PIA scope> processing*

**Personally Identifiable Information (PII)**

<table>
<thead>
<tr>
<th>Data Item</th>
<th>Data Item Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.</td>
<td></td>
</tr>
<tr>
<td>15.</td>
<td></td>
</tr>
<tr>
<td>16.</td>
<td></td>
</tr>
<tr>
<td>17.</td>
<td></td>
</tr>
<tr>
<td>18.</td>
<td></td>
</tr>
<tr>
<td>19.</td>
<td></td>
</tr>
<tr>
<td>20.</td>
<td></td>
</tr>
<tr>
<td>21.</td>
<td></td>
</tr>
<tr>
<td>22.</td>
<td></td>
</tr>
<tr>
<td>23.</td>
<td></td>
</tr>
<tr>
<td>24.</td>
<td></td>
</tr>
<tr>
<td>25.</td>
<td></td>
</tr>
<tr>
<td>26.</td>
<td></td>
</tr>
</tbody>
</table>

*Figure 2 – Data Within <Company X><PIA scope> Processing*

**Areas of concern**

*fill in*

**Recommendations**

*fill in*

3. Privacy Complaints and Incidents

*Put description of review and work here.*
4. Privacy Policies and Practices

4.1 Website Privacy Policies

<Put description of work and review here>

Areas of concern
<fill in>

Recommendations
<fill in>

4.2 Internal Information Security and Privacy Policies

<Describe importance of policies and procedures here>

<Describe work, research and findings here>

Areas of concern
<fill in>

Recommendations
<fill in>
5. Privacy Programs and Executive Support

<Company X> <provide applicable information here>

<table>
<thead>
<tr>
<th>Areas of concern</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;fill in&gt;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;fill in&gt;</td>
</tr>
</tbody>
</table>

6. Awareness and Training

<Company X> <provide applicable information here>

<table>
<thead>
<tr>
<th>Areas of concern</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;fill in&gt;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;fill in&gt;</td>
</tr>
</tbody>
</table>

7. PII Collection and Access

<Background>

7.1 Customer PII Collection
Customer PII is collected within <Company X> through the <Company X><PIA scope>.

- The <Company X><PIA scope> <provide applicable information here> The data items are listed in Table 2. PII items are highlighted in green. Information that, when coupled with a PII item, becomes sensitive are highlighted in yellow.

<table>
<thead>
<tr>
<th>Data Item</th>
<th>Data Item Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td></td>
</tr>
</tbody>
</table>
Table 2 – Data Within <Company X><PIA scope> Processing

<Illustrations> <Company X><PIA scope> looks on a website.  
<Include diagrams, illustrations, screen prints, etc. as appropriate to the PIA scope.>

<Describe all types of PII collection activities here>

7.2 Use Limitation & Sharing Customer PII With Third Parties  
<Background>

<Describe PII sharing practices here>

7.3 Purpose Specification
Describe how purposes for PII use are, or are not, provided:

**Areas of concern**

<fill in>

**Recommendations**

<fill in>

### 7.4 Individual Participation

Describe how individuals can access their own PII:

**Areas of concern**

<fill in>

**Recommendations**

<fill in>

### 8. Customer PII Storage

Describe PII storage practices and locations:

**Areas of concern**

<fill in>

**Recommendations**

<fill in>

### 9. Laws, Regulations and Contracts
10. Contractual Obligations

Areas of concern
<fill in>

Recommendations
<fill in>

11. Background checks

<Description>
12. Safeguards & Data Integrity

<Company X> has <include information here as appropriate>

13. Data Quality

The <Company X><PIA scope> <include information here as appropriate>

14. Customer PII Used for Test Purposes
Currently production <Company X> customer PII is <provide details as applicable here>

**Areas of concern**

<fill in>

**Recommendations**

<fill in>

15. Limiting access within applications and systems

<Company X> controls access to customer PII through <provide applicable details here>

**Areas of concern**

<fill in>

**Recommendations**

<fill in>

16. Oversight, Maintenance & Evaluation

**16.1 Accountability**

The <Company X> <provide applicable details here>
16.2 Openness

<Company X> <provide applicable details here>

Areas of concern

<fill in>

Recommendations

<fill in>

16.3 Customer PII Retention

<Company X> <provide applicable details here>

Areas of concern

<fill in>

Recommendations

<fill in>
16.4 Customer PII Disposal

The <Company X> <include applicable information here>

Areas of concern

<fill in>

Recommendations

<fill in>

16.5 Compliance and enforcement

<Company X> <include applicable information here>

Areas of concern

<fill in>

Recommendations

<fill in>
Appendix A – <Company X> Privacy Survey Responses

<Put verbatim copies of completed PIA surveys here>
Appendix B – Existing <Company X> Information Security and Privacy Policies

<Fill in as appropriate>
Appendix C – Recommended Information Security and Privacy Policies & Supporting Documents

<Fill in as appropriate>
Appendix D – <Company X> PIA Project Meeting Notes

Copy all PIA meeting notes here
Appendix E – U.S. State Breach Notice Laws

© 2009 Rebecca Herold & Associates, LLC. All rights reserved.
Appendix F – <Company X> Website Privacy Policies

<Copy here verbatim>
Appendix G - Data Protection (Privacy) Laws

<Describe applicable laws here>
Appendix H - <Company X> Information Security and Privacy Training and Awareness Program

<Fill in as appropriate>
Appendix I - Recommended \textit{<Company X>Website Privacy Policy}

\textit{<Fill in appropriately>
Appendix J - Updated `<Company X>` Website Privacy Policy

<Fill in as applicable>
Appendix K – <Change to PIA Specific Issue>
Appendix L – <Change to PIA Specific Issue>
Appendix M – Updated <Company X> Security Policies

<Change appropriately>