



 **ERNST & YOUNG**

*Quality In Everything We Do*

**Phorm, Inc.**

**Phorm Service**

**Privacy Examination Report**

**January 2008**

# Contents

Audit Approach and Communications .....	1
The Ernst & Young Project Approach and Scope .....	1
Management's Controls Description .....	2
2007 Audit Results .....	3
Report of Independent Accountants .....	3
Report of Phorm Management's Privacy Controls over the Phorm Service .....	4
Appendix A: Phorm Service Privacy Policy .....	5
Appendix B: AICPA Generally Accepted Privacy Principles.....	8

# Audit Approach and Communications

## The Ernst & Young Project Approach and Scope

Ernst & Young LLP (“E&Y”) performed an examination of Phorm, Inc.’s Service (Service) regarding the collection, use, retention, and disclosure of information according to the AICPA Generally Accepted Privacy Principles. This service was provided in accordance with the applicable AICPA Professional Standards, including the Statement on Standards for Attestation Engagements (SSAE) Number 10 and the Standards for Consulting. As part of such examination, Phorm (the Company), with the advice of E&Y, defined the assertions in accordance with the AICPA Generally Accepted Privacy Principles and the Company’s privacy policies (the “Assertions”). E&Y determined whether the Assertions set forth in the Examination Report (as hereinafter defined) are fairly stated, in all material respects, based on the criteria and whether the Assertions are complete and sufficient to satisfy the Company’s privacy policies and meet the AICPA Generally Accepted Privacy Principles.

Specifically, the scope of this engagement included the following subjects related to the Service:

- **Management.** How the Company defines, documents, communicates, assigns and assesses the effectiveness of its security and privacy policies and procedures.
- **Technical.** How the Company has implemented a technical system design with effective controls in accordance with the established criteria.
- **Security.** How the Company protects information against unauthorized access (both physical and logical) and detects such incident for internal and external security response purposes.
- **Quality.** How the Company maintains accurate, complete, and relevant information for the purposes identified in the security and privacy policies.
- **Monitoring and Enforcement.** How the Company monitors compliance with its security privacy policies and procedures and has procedures to address privacy-related complaints and disputes.

The scope of our examination does not include any components or personnel of the Company that are not under direct control of the Company or that the Company has access to via a contractual relationship.

The specific criteria of the AICPA Generally Accepted Privacy Principles can be seen in [Appendix B](#).

# Management's Controls Description



Liberty House  
222 Regent Street  
Second Floor  
London W1B 5TR  
T +44 (0)207 297 2067  
F +44 (0)207 297 2161

264 W 40<sup>th</sup> Street  
16th Floor  
New York, NY 10018  
T +1 212 359 2030  
F +1 212 938 0131

[www.phorm.com](http://www.phorm.com)

To All,

Privacy is of the utmost importance to Phorm and we are committed to protecting the privacy of Internet users. As such, we commissioned Ernst & Young to conduct an independent examination of our systems and assertions as part of this commitment. The following components of our privacy program were examined by our auditors:

- ◆ Phorm's privacy policy, controls and procedures
- ◆ Phorm's compliance with its stated privacy policy
- ◆ Phorm employees' privacy policy training and compliance
- ◆ Data retention, integrity and security policies and procedures.

We are pleased that the attached attestation report confirms that Phorm's systems have been found to be designed specifically to protect the identity and other sensitive information of consumers in the following key ways:

## **I. Phorm's systems do not use or intentionally store or collect personally identifiable information from consumers.**

Phorm is able to do this as Phorm's systems:

- Do not tie into the authentication systems of our ISP partners;
- Do not store the IP address, which is potentially another mechanism to identify a consumer household;
- Ignore information such as form fields, numbers with more than 3 digits (to protect against the accidental collection of social security, telephone and credit card numbers), email addresses and secure (HTTPS) pages.

## **II. Phorm has established industry-leading standards regarding storage, retention and deletion of data.**

Storage, retention and use of consumer data are currently key concerns in the online advertising industry. Phorm's systems collect browsing information such as URLs visited, search terms entered, OS version, relevant keywords of a particular page and randomly-generated unique IDs. Importantly, however:

- This specific data cannot be accessed by our ISP partners.
- Even this non-personally-identifiable information is automatically purged from the production system immediately. (Research and debug logs may be kept on a separate system for a maximum of 14 days).
- Once the system purges this data, it is not possible for us to release it, either accidentally or deliberately.

## **III. An Easy Opt-Out Mechanism**

We offer an easy, anonymous method for users to opt out of Phorm's systems if they would rather not receive targeted advertising and content. For as long as a user retains the Phorm opt-out cookie, the system will not collect or store data on their browsing behavior.

Please see the full Ernst & Young attestation letter, attached, for their full statement.

Sincerely,

A handwritten signature in blue ink, appearing to read "Kent Ertugrul".

Kent Ertugrul  
CEO  
Phorm, Inc.



# 2007 Audit Results



■ Ernst & Young LLP  
5 Times Square  
New York, NY 10036

■ Phone: (212) 773-3000  
Fax: (212) 773-6350  
[www.ey.com](http://www.ey.com)

## Report of Independent Accountants

### To the Management of Phorm, Inc.:

We have examined Phorm, Inc.'s ("Phorm") management assertion that during the period of June 1, 2007 through December 15, 2007 it:

- Maintained effective controls over the privacy of personal information collected in its Phorm Service (Service) to provide reasonable assurance that the personal information was collected, used, retained, and disclosed in conformity with its commitments in its privacy policy and with criteria set forth in Generally Accepted Privacy Principles, issued by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA), and
- Complied with its commitments in the privacy policy.

This assertion is the responsibility of Phorm's management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the AICPA and, accordingly, included (1) obtaining an understanding of Phorm's controls over the privacy of personal information collected in the Service, (2) testing and evaluating the operating effectiveness of the controls, (3) testing compliance with Phorm's commitments in its privacy policy, and (4) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of inherent limitations in controls, error or fraud may occur and not be detected.

Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the Service or controls, the failure to make needed changes to the Service or controls, or a deterioration in the degree of effectiveness of the controls.

In our opinion, Phorm's management assertion referred to above is fairly stated, in all material respects, in conformity with Phorm's privacy policy and with the criteria set forth in the AICPA Generally Accepted Privacy Principles.

*Ernst & Young LLP*

New York, NY  
December 15, 2007  
[www.ey.com/us](http://www.ey.com/us)

## Report of Phorm Management's Privacy Controls over the Phorm Service

At Phorm, we are deeply committed to the privacy and security rights of individuals. Our technology and systems have been designed and built specifically to protect the identity and other sensitive information of consumers while delivering tailored content and advertising. Furthermore, we want to make sure that Internet users feel comfortable with what we do. To that end, we explain our approach on our company website, and have created an extensive privacy policy ([See Appendix A](#)) that outlines the fair handling of personal information and have established an array of privacy protection mechanisms.

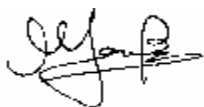
To actively demonstrate our commitment to these core principles and assertions we make, we have undergone an independent, third party examination of our privacy commitments and controls. We have engaged Ernst & Young LLP, a global professional services organization, to examine and report on our compliance with our privacy policy.

Specifically, as the management of the Phorm Service (Service), we are responsible for establishing and maintaining effective controls over the privacy of personal information that our systems collect. The controls that we have established have been designed to provide reasonable assurance that the information is protected in conformity with our disclosed privacy practices. These controls contain monitoring mechanisms and actions are taken to correct deficiencies identified, if any.

There are inherent limitations in any controls, including the possibility of human error and the circumvention or overriding of controls. While even effective controls can provide only reasonable assurance, we have taken a great deal of effort to mitigate such limitations. Because of potential changes in conditions, we will continue to monitor the effectiveness of controls over time to prevent any degradation.

Management at Phorm has assessed the controls over the Service. Based on that assessment, in Phorm management's opinion, in providing the Service, during the period June 1, 2007 through December 15, 2007, Phorm has:

- Maintained effective controls over the privacy of personal information collected in the Phorm Service (Service) to provide reasonable assurance that the personal information was collected, used, retained and disclosed in conformity with our commitments in our privacy policy related to the Service and to enable Ernst & Young to validate conformance and with the criteria set forth in Generally Accepted Privacy Principles, issued by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA), and
- Complied with our commitments in our privacy policy.



Marc Burgess, SVP Technology  
December 15, 2007



Liberty House  
222 Regent Street  
Second Floor  
London W1B 5TR  
T +44 (0)207 297 2067  
F +44 (0)207 297 2161

264 W 40<sup>th</sup> Street  
16th Floor  
New York, NY 10018  
T +1 212 359 2030  
F +1 212 938 0131

[www.phorm.com](http://www.phorm.com)

## Appendix A: Phorm Service Privacy Policy

Phorm, Inc. provides the Phorm Service for Internet service providers ("ISPs"), advertisers, networks and publishers. The Phorm Service is a patent-pending technology that delivers targeted advertising and consumer services to ISP customers ("Users") on behalf of Phorm, our partner ISPs and affiliated websites.

At Phorm, consumer privacy is of paramount importance. Phorm has spent years designing a system that is industry leading in terms of consumer privacy protection. This document details how the Phorm Service works and how non-personally identifiable information (described below) may be used to make the internet safer and more relevant for consumers. Our claims have been verified by independent auditor, Ernst & Young, to give consumers level of comfort that this Privacy Policy statement is true and accurate. The Phorm Service is designed to provide consumers with a safer and more relevant Internet, and Phorm fully believes in giving consumers choice. To that end, Phorm offers consumers a simple mechanism for them to switch the Phorm Service on or off, which we explain below.

### What information does Phorm Service collect?

The Phorm Service is designed to avoid collection of any Personally Identifiable Information of the user ("PII"), namely information that can be directly associated with that specific person or entity, e.g. a name, a postal address, a phone number, or an email. Phorm Service uses only Non-Personally Identifiable Information ("non-PII"), such as search terms, URLs and keywords. Phorm Service does not store or retain this information. This information is used to understand broad categories of that consumer's interests; the Phorm Service matches this with existing advertising categories ("category match"), then immediately discards this information. It is important for consumers to know that even the limited retained category match information cannot be used to identify any specific person or entity. By way of example, Phorm Service will retain only information about general categories of interest associated with a randomly generated ID (category matches) such as "ID #45678 is interested in IPODs."

Phorm Service also uses "cookies," a small text file stored on the hard drive of a user's computer to enable Phorm and other Web entities to anonymously identify repeat users. The Phorm cookie is 'blind' to users' identities, because Phorm only use a randomly generated ID number to identify the cookie associated with the computer. Phorm Service uses cookies to communicate with its servers in order to limit how often ads are displayed, and to help to decide which ads to display. The cookies used by Phorm Service contain no PII.

### How is the Phorm Service designed to not collect PII?

Phorm takes several steps in designing the Phorm Service to not collect any PII. For example, Phorm Service:

- Does not collect any information on secure (HTTPS) pages.
- Does not collect information that users enter in web form fields such as registration pages.
- Ignores words or phrases containing the "@" symbol to ensure that we do not collect email addresses.
- Ignores numbers longer than three digits, to prevent the collection of credit card numbers, phone numbers, social security numbers, or other numbers-based PII.
- Does not store IP addresses.

If any PII were collected, Phorm would be legally obliged to use any information in line with the applicable laws concerning protection of such information.

### **How do you use the information you collect?**

Phorm Service may use the information it gathers to give users warnings and alerts about websites they may be visiting, and to provide information about goods and services that may interest them, based on the websites they are visiting and the search terms they are using.

For example, visits to a travel website suggest an interest in the topic 'travel'. Phorm Service records those category matches in order to place ads that may be of interest to that user. After making a category match, all of the information (which contains no PII) leading to the category match is purged from the Phorm system.

This is an important point: because Phorm Service does not permanently store the non-PII or IP addresses, it is incapable of identifying any specific person or entity.

### **Do you share information with third parties?**

Phorm may share aggregated advertising category match information to provide statistics to partner ISPs, prospective clients and business partners. We will not disclose any randomly generated ID associated with a cookie to any third party, which means that none of this shared information can be used to identify individual users.

For example, Phorm may tell a merchant that our network contains 50,000 users who have visited a travel website URL in the past six months, but cannot disclose which randomly generated IDs have visited that URL, because that information is simply not stored.

If legally required to do so, Phorm will disclose to a third party any information it does have, but as stated above our Phorm Service is designed not to collect or retain any such information.

### **How can users opt-out of Phorm Service?**

The Phorm Service website provides users with a simple opt-out form. Users who opt-out will receive an opted-out cookie that prevents Phorm Service from using any information at all from the specific browser associated with that computer.

If a user deletes their opt-out cookie, then the opt-out status, which is contained in the cookie, is lost, and the user will be opted-back into the Phorm Service. The reason that Phorm employs a cookie-based opt-out is to ensure that such opt-out is effective no matter where a consumer may take his or her computer and is in other ways more protective of a consumer's identity. If you delete your cookies and still would like to be opted-out of the Phorm Service, please return to the website and opt-out again. (This is an industry standard practice, as described on the NAI site, [www.networkadvertising.org](http://www.networkadvertising.org)).

In addition, users may be able to prevent cookies from any website from being installed on their computer by readjusting their browser settings. For more information on cookies and how to disable them, users should consult the Help section of their browser. Alternatively, users can consult the information provided by the Interactive Advertising Bureau at [www.allaboutcookies.org](http://www.allaboutcookies.org).

### **What does this privacy policy not cover?**

This privacy policy applies to the Phorm Service only and does not apply to other features or services provided by Phorm's partner ISPs or other third parties. To better understand the privacy practices of your ISP or another third party, we encourage you to review their privacy policy and user agreements.



### **Can I find out what PII Phorm Service keeps about me?**

The Phorm Service is designed to avoid the collection and storage of PII, however you have the right to request a copy of any information that Phorm may have about you and to have any inaccuracies corrected. A reasonable fee may be charged for information requests, and we reserve the right to request such evidence as we consider reasonably necessary in the circumstances to prove your identity. We will use reasonable efforts to supply, correct or delete any information about you that Phorm may have.

For more information, please contact:

The Data Protection Officer  
222 Liberty House  
London W1B 5TR  
[dataprotectionofficer@Phorm.com](mailto:dataprotectionofficer@Phorm.com)

### **What are Phorm's security practices?**

Phorm has implemented security measures to protect information collected on this website from loss, misuse, unauthorized access, disclosure, alteration or destruction. Our employees are made aware of and must comply with these procedures.

Please keep in mind, however, that the Internet is not a 100% secure medium. Therefore, it is theoretically possible that somebody could defeat our security measures. However, as stated above, none of the information could identify you or any other individual.

We sometimes use third-party contractors to perform tasks that might otherwise be done by our employees. These contractors, however, are contractually bound to adhere to this privacy policy, and they are subject to similar restrictions as our employees.

If you use your computer and usual browser in a country other than your home country to log on to the Internet via one of our partner ISPs in that other country, the data that Phorm holds in its system that is associated with that cookie may be automatically transferred to Phorm's systems in that other country.

### **Changes to our privacy policy**

The Phorm privacy policy may be updated from time to time, and the most current versions can be found at [http://www.phorm.com/user\\_privacy](http://www.phorm.com/user_privacy).

## Appendix B: AICPA Generally Accepted Privacy Principles

Control Ref.	AICPA Privacy Framework Criterion
<b>1.0 Management</b>	
1.1.0	<b>Privacy Policies</b> The entity defines and documents its privacy policies with respect to: <ul style="list-style-type: none"> <li>• Notice (<a href="#">See 2.1.0</a>)</li> <li>• Choice and <a href="#">Consent</a> (<a href="#">See 3.1.0</a>)</li> <li>• Collection (<a href="#">See 4.1.0</a>)</li> <li>• Use and Retention (<a href="#">See 5.1.0</a>)</li> <li>• Access (<a href="#">See 6.1.0</a>)</li> <li>• Onward Transfer and Disclosure (<a href="#">See 7.1.0</a>)</li> <li>• Security (<a href="#">See 8.1.0</a>)</li> <li>• Quality (<a href="#">See 9.1.0</a>)</li> <li>• Monitoring and Enforcement (<a href="#">See 10.1.0</a>)</li> </ul>
1.1.1	<b>Communication to Internal Personnel</b> Privacy policies and the consequences of noncompliance with such policies are communicated at least annually to the entity's internal personnel responsible for collecting, using, retaining, and disclosing <a href="#">personal information</a> . Changes in privacy policies are communicated to such personnel shortly after the changes are approved.
1.1.2	<b>Responsibility and Accountability for Policies</b> Responsibility and accountability are assigned to a person or group for documenting, implementing, enforcing, monitoring, and updating the entity's privacy policies. The names of such person or group and their responsibilities are communicated to internal personnel.
1.2.1	<b>Review and Approval</b> Privacy policies and procedures and changes thereto are reviewed and approved by management.
1.2.2	<b>Consistency of Privacy Policies and Procedures With Laws and Regulations</b> Policies and procedures are reviewed and compared to the requirements of applicable laws and regulations at least annually and whenever there are changes to such laws and regulations. Privacy policies and procedures are revised to conform with the requirements of applicable laws and regulations.
1.2.3	<b>Consistency of Commitments With Privacy Policies and Procedures</b> Entity personnel or advisors review contracts for consistency with privacy policies and procedures and address any inconsistencies.
1.2.4	<b>Infrastructure and Systems Management</b> Entity personnel or advisors review the design, acquisition, implementation, configuration, and management of the infrastructure, systems, and procedures and changes thereto for consistency with the entity's privacy policies and procedures and address any inconsistencies.
1.2.5	<b>Supporting Resources</b> Resources are provided by the entity to implement and support its privacy policies.

## PHORM SERVICE PRIVACY EXAMINATION REPORT

Control Ref.	AICPA Privacy Framework Criterion
1.2.6	<b>Qualifications of Personnel</b> The entity establishes qualifications for personnel responsible for protecting the privacy and security of personal information and assigns such responsibilities only to those personnel who meet these qualifications and have received needed training.
1.2.7	<b>Changes in Business and Regulatory Environments</b> For each jurisdiction in which the entity operates, the effect on privacy of changes in the following factors is identified and addressed: <ul style="list-style-type: none"> <li>* Business operations and processes</li> <li>* People</li> <li>* Technology</li> <li>* Legal</li> <li>* Contracts, including service-level agreements</li> </ul> Privacy policies and procedures are updated for such changes.
<b>2.0 Notice</b>	
2.1.0	<b>Privacy Policies</b> The entity's privacy policies address providing notice to <a href="#">individuals</a> .
2.1.1	<b>Communication to Individuals</b> Notice is provided to individuals regarding the following privacy policies: <ul style="list-style-type: none"> <li>• Purpose for collecting personal information</li> <li>• Choice and Consent (<a href="#">See 3.1.1</a>)</li> <li>• Collection (<a href="#">See 4.1.1</a>)</li> <li>• Use and Retention (<a href="#">See 5.1.1</a>)</li> <li>• Access (<a href="#">See 6.1.1</a>)</li> <li>• Onward Transfer and Disclosure (<a href="#">See 7.1.1</a>)</li> <li>• Security (<a href="#">See 8.1.1</a>)</li> <li>• Quality (<a href="#">See 9.1.1</a>)</li> <li>• Monitoring and Enforcement (<a href="#">See 10.1.1</a>)</li> </ul> If personal information is collected from sources other than the individual, such sources are described in the notice.
2.2.1	<b>Provision of Notice</b> Notice is provided to the individual about the entity's privacy policies and procedures: <ul style="list-style-type: none"> <li>• At or before the time personal information is collected, or as soon as practical thereafter.</li> <li>• At or before the entity changes its privacy policies and procedures, or as soon as practical thereafter</li> <li>• Before personal information is used for new purposes not previously identified (<a href="#">See 3.2.2, "Consent for New Purposes and Uses."</a>)</li> </ul>
2.2.2	<b>Entities and Activities Covered</b> An objective description of the entities and activities covered by the privacy policies and procedures is included in the entity's privacy notice.
2.2.3	<b>Clear and Conspicuous</b> Clear and conspicuous language is used in the entity's privacy notice.
<b>3.0 Choice and Consent</b>	
3.1.0	<b>Privacy Policies</b> The entity's privacy policies address the choices available to individuals and the consent to be obtained.

## PHORM SERVICE PRIVACY EXAMINATION REPORT

Control Ref.	AICPA Privacy Framework Criterion
3.1.1	<b>Communication to Individuals</b> Individuals are informed: <ul style="list-style-type: none"> <li>About the choices available to them with respect to the collection, use, and disclosure of personal information.</li> </ul> That implicit or explicit consent is required to collect, use, and disclose personal information, unless a law or regulation specifically requires otherwise.
3.1.2	<b>Consequences of Denying or Withdrawing Consent</b> When personal information is collected, individuals are informed of the consequences of refusing to provide personal information or of denying or withdrawing consent to use personal information for purposes identified in the notice.
3.2.1	<b>Implicit or Explicit Consent</b> Implicit or explicit consent is obtained from the individual at or before the time personal information is collected or as soon as practical thereafter. The individual's preferences expressed in his or her consent are confirmed and implemented.
3.2.2	<b>Consent for New Purposes and Uses</b> If information that was previously collected is to be used for purposes not previously identified in the privacy notice, the new purpose is documented, the individual is notified, and implicit or explicit consent is obtained prior to such new use or purpose.
3.2.3	<b>Explicit Consent for Sensitive Information</b> Explicit consent is obtained directly from the individual when sensitive personal information is collected, used, or disclosed, unless a law or regulation specifically requires otherwise.
3.2.4	<b>Consent for Online Data Transfers to/from an Individual's Computer</b> Consent is obtained before personal information is transferred to/from an individual's computer.
<b>4.0 Collection</b>	
4.1.0	<b>Privacy Policies</b> The entity's privacy policies address the collection of personal information.
4.1.1	<b>Communication to Individuals</b> Individuals are informed that personal information is collected only for the purposes identified in the notice.
4.1.2	<b>Types of Personal Information Collected and Methods of Collection</b> The types of personal information collected and the methods of collection, including the use of <u>cookies</u> or other tracking techniques, are documented and described in the privacy notice.
4.2.1	<b>Collection Limited to Identified Purpose</b> The collection of personal information is limited to that necessary for the purposes identified in the notice.
4.2.2	<b>Collection by Fair and Lawful Means</b> Methods of collecting personal information are reviewed by management, legal counsel, or both before they are implemented to confirm that personal information is obtained: <ul style="list-style-type: none"> <li>Fairly, without intimidation or deception, and</li> <li>Lawfully, adhering to all relevant rules of law, whether derived from statute or common law, relating to the collection of personal information</li> </ul>
4.2.3	<b>Collection From Third Parties</b> Management confirms that third parties from whom personal information is collected (that is, sources other than the individual) are reliable sources that collect information fairly and lawfully.
<b>5.0 Use and Retention</b>	
5.1.0	<b>Privacy Policies</b> The entity's privacy policies address the use and retention of personal information.

## PHORM SERVICE PRIVACY EXAMINATION REPORT

Control Ref.	AICPA Privacy Framework Criterion
5.1.1	<b>Communication to Individuals</b> Individuals are informed that personal information is: <ul style="list-style-type: none"> <li>Used only for the purposes identified in the notice and only if the individual has provided implicit or explicit consent, unless a law or regulation specifically requires otherwise.</li> <li>Retained for no longer than necessary to fulfill the stated purposes, or for a period specifically required by law or regulation.</li> </ul>
5.2.1	<b>Use of Personal Information</b> Personal information is used only for the purposes identified in the notice and only if the individual has provided implicit or explicit consent, unless a law or regulation specifically requires otherwise.
5.2.2	<b>Retention of Personal Information</b> Personal information is retained for no longer than necessary to fulfill the stated purposes unless a law or regulation specifically requires otherwise. Personal information no longer retained is disposed and destroyed of in a manner that prevents loss, misuse, or unauthorized access.
<b>6.0 Access</b>	
6.1.0	<b>Privacy Policies</b> The entity's privacy policies address providing individuals with access to their personal information.
6.1.1	<b>Communication to Individuals</b> Individuals are informed about how they may obtain access to their personal information to review, update, and correct that information.
6.2.1	<b>Access by Individuals to Their Personal Information</b> Individuals are able to determine whether the entity maintains personal information about them and, upon request, may obtain access to their personal information.
6.2.2	<b>Confirmation of an Individual's Identity</b> The identity of individuals who request access to their personal information is authenticated before they are given access to that information.
6.2.3	<b>Understandable Personal Information, Time Frame, and Cost</b> Personal information is provided to the individual in an understandable form, in a reasonable time frame, and at a reasonable cost, if any.
6.2.4	<b>Denial of Access</b> Individuals are informed, in writing, of the reason a request for access to their personal information was denied, the source of the entity's legal right to deny such access, if applicable, and the individual's right, if any, to challenge such denial, as specifically permitted or required by law or regulation.
6.2.5	<b>Updating or Correcting Personal Information</b> Individuals are able to update or correct personal information held by the entity. If practical and economically feasible to do so, the entity provides such updated or corrected information to third parties that previously were provided with the individual's personal information.
6.2.6	<b>Statement of Disagreement</b> Individuals are informed, in writing, about the reason a request for correction of personal information was denied, and how they may appeal.
6.2.7	<b>Escalation of Complaints and Disputes</b> Complaints and other disputes are escalated until they are resolved.
<b>7.0 Onward Transfer and Disclosure</b>	
7.1.0	<b>Privacy Policies</b> The entity's privacy policies address the disclosure of personal information to third parties.



## PHORM SERVICE PRIVACY EXAMINATION REPORT

Control Ref.	AICPA Privacy Framework Criterion
7.1.1	<b>Communication to Individuals</b> Individuals are informed that personal information is disclosed to third parties only for the purposes identified in the notice and for which the individual has provided implicit or explicit consent unless a law or regulation specifically allows or requires otherwise. Disclosure includes any limitation on the third party's privacy practices and controls. Lack of such disclosure indicates that the third party's privacy practices and controls meet or exceed those of the entity.
7.1.2	<b>Communication to Third Parties</b> Privacy policies are communicated to third parties to whom personal information is disclosed.
7.2.1	<b>Disclosure of Personal Information</b> Personal information is disclosed to third parties only for the purposes described in the notice and for which the individual has provided implicit or explicit consent, unless a law or regulation specifically allows or requires otherwise.
7.2.2	<b>Protection of Personal Information</b> Personal information is disclosed only to third parties who have agreements with the entity to protect personal information from loss, misuse, unauthorized access, disclosure, alteration, and destruction.
7.2.3	<b>New Purposes and Uses</b> Personal information is disclosed to third parties for new purposes or uses only with the prior implicit or explicit consent of the individual.
7.2.4	<b>Misuse of Personal Information by a Third Party</b> The entity takes remedial action in response to misuse of personal information by a third party to whom the entity has transferred such information.
<b>8.0 Security</b>	
8.1.0	<b>Privacy Policies</b> The entity's privacy policies address the security of personal information.
8.1.1	<b>Communication to Individuals</b> Individuals are informed that precautions are taken to protect personal information.
8.2.1	<b>Information Security Program</b> A security program has been developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect personal information from loss, misuse, unauthorized access, disclosure, alteration, and destruction.
8.2.2	<b>Logical Access Controls</b> Logical access to personal information is restricted by procedures that address the following matters: <ul style="list-style-type: none"> <li>a. Authorizing and registering internal personnel and individuals</li> <li>b. Identifying and authenticating internal personnel and individuals</li> <li>c. Making changes and updating access profiles</li> <li>d. Granting system access privileges and permissions</li> <li>e. Preventing individuals from accessing other than their own personal or sensitive information</li> <li>f. Limiting access to personal information to only authorized internal personnel based upon their assigned roles and responsibilities</li> <li>g. Distributing output only to authorized internal personnel</li> <li>h. Restricting logical access to offline storage, backup data, systems, and media</li> <li>i. Restricting access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls)</li> <li>j. Preventing the introduction of viruses, malicious code, and unauthorized software.</li> </ul>
8.2.3	<b>Physical Access Controls</b> Physical access is restricted to personal information in any form (including the components of the entity's system(s) that contain or protect personal information).

## PHORM SERVICE PRIVACY EXAMINATION REPORT

Control Ref.	AICPA Privacy Framework Criterion
8.2.4	<b>Environmental Safeguards</b> Personal information, in all forms, is protected against unlawful destruction, accidental loss, natural disasters, and environmental hazards.
8.2.5	<b>Transmitted Personal Information</b> Personal information is protected when transmitted by mail and over the Internet and public networks by deploying industry standard encryption technology for transferring and receiving personal information.
8.2.6	<b>Testing Security Safeguards</b> Tests of the effectiveness of the key administrative, technical, and physical safeguards protecting personal information are conducted at least annually.
<b>9.0 Quality</b>	
9.1.0	<b>Privacy Policies</b> The entity's privacy policies address the quality of personal information.
9.1.1	<b>Communication to Individuals</b> Individuals are informed that they are responsible for providing the entity with accurate and complete personal information, and for contacting the entity if correction of such information is required.
9.2.1	<b>Accuracy and Completeness of Personal Information</b> Personal information is accurate and complete for the purposes for which it is to be used.
9.2.2	<b>Relevance of Personal Information</b> Personal information is relevant to the purposes for which it is to be used.
<b>10.0 Monitoring and Enforcement</b>	
10.1.0	<b>Privacy Policies</b> The entity's privacy policies address the monitoring and enforcement of privacy policies and procedures.
10.1.1	<b>Communication to Individuals</b> Individuals are informed about how to contact the entity with complaints.
10.2.1	<b>Complaint Process</b> A process is in place to address complaints.
10.2.2	<b>Dispute Resolution and Recourse</b> Every complaint is addressed and the resolution is documented and communicated to the individual.
10.2.3	<b>Compliance Review</b> Compliance with privacy policies and procedures, commitments and applicable laws, regulations, service-level agreements, and other contracts is reviewed and documented and the results of such reviews are reported to management. If problems are identified, the entity's privacy policies and procedures are enforced.
10.2.4	<b>Instances of Noncompliance</b> Instances of noncompliance with privacy policies and procedures are documented and reported and, if needed, corrective measures are taken on a timely basis.