Association of Clinical Research Professionals
Finance Committee Policy 4.7

Information Security Breach Notification

Purpose
The purpose of the Information Security Breach Notification Policy (the "Policy") is to ensure the security and timely notification of any breaches to the personal and proprietary data of the Association of Clinical Research Professionals (ACRP) and its "customers" (members, affiliates, business partners and other groups or individuals engaged with the business of the association.) The goal is to prevent identity theft and fraud and to protect the association's business integrity and reputation.

Authority
The Executive Director is responsible for ensuring the data security of ACRP and its customers.

Administration
The Executive Director and Senior Director, Operations shall be responsible for developing, implementing and revising this policy in consultation with technology staff and/or IT consultants.

Policy
Personally Identifiable Information (PII) -

'PII' is used in this and all ACRP Security Policies. It is defined as: 'Any data, including financial information, that could potentially identify a specific individual.'

PII Risk Assessment

When a suspected security or privacy incident occurs, a risk assessment will be performed by a third-party vendor or IT management contractor in conjunction with the Senior Director, Operations to determine whether PII has been compromised. The following four objective factors will be used in the risk assessment:

1. The nature and extent of the PII involved.
2. The unauthorized person who used the PII or to whom the impermissible disclosure was made.
3. Whether the PII was actually acquired or viewed or, alternatively, if only the opportunity existed for the information to be acquired or viewed.
4. The extent to which the risk to the PII has been mitigated.

Breach Notification

Once a PII breach is identified, ACRP will provide notification to its customers about the breach without unreasonable delay. The notification will include information on the nature of the breach and steps that have

been taken to mitigate risk. Where applicable, the notification will also provide customers with follow-up instructions such as whether to change passwords or if other accounts may be at risk.

Workforce Training

ACRP will re-train all workforce members who caused or created the conditions that allowed the breach to occur. If misconduct is suspected, ACRP will apply disciplinary actions according to its personnel policies. (See Workplace Conduct (5-1) and Use of Communications and Computers (5-5) in the ACRP Employee Handbook.)

Documentation

ACRP will thoroughly document all breach-related activities and investigations in a timely manner to provide a historic accounting and to provide guidance on how to reduce future risk.

MONITORING AND REVIEW SCHEDULE

Review every three years by the Executive Director and Senior Director, Operations in consultation with technology staff and/or IT consultants.

DATES REVIEWED
December 13, 2017 (by ABoT)

DATES MODIFIED
December 13, 2017 (By ABoT)

DATES APPROVED
December 13, 2017 (By ABoT)