SECURITY EXHIBIT

This Security Exhibit shall be incorporated into the Purchase Order Terms and Conditions between the parties. In the event that the Supplier has executed a Business Associates Agreement to comply with the Health Insurance Portability and Accountability Act of 1996, Public Law 104 191 ("HIPAA"), the Privacy Rule, the Security Rule and HITECH, the Business Associates Agreement shall control in the event of a conflict between this Security Exhibit and the Business Associates Agreement.

1. Security Program. During the term of the Agreement, the Supplier shall maintain and implement a formal security program in accordance with industry standards (the "Security Program") that is designed to (i) ensure the security, Confidentiality and Integrity of Mosaic's data or information ("Mosaic Data") developed, received, accessed, or acquired by the Supplier in performance of the services and all derivatives thereof, (ii) protect against threats or hazards to the security, Confidentiality and Integrity of Mosaic Data; and (iii) prevent unauthorized access to Mosaic Data. Without limiting the scope of this Security Exhibit, the Supplier shall require its employees, agents, representatives, subcontractors, and any other party engaged by the Supplier in support of the services provided to Mosaic ("Supplier Parties") to agree in writing to be bound by security terms no less restrictive than those contained in this Agreement, and the Supplier shall be liable for the compliance of such Supplier Parties. The Security Program applies to the business computing environment of the Supplier and the Supplier Parties in which Mosaic Data is stored, accessed or otherwise processed.

2. Unauthorized Disclosure. If either party believes that there has been a disclosure of Mosaic Data to anyone other than the Supplier or Supplier Parties, such party must promptly notify the other party. If either party intends to notify third parties of such disclosure of Mosaic Data, prior to such third-party notification, such party shall provide the other party written notice of such intent. Additionally, each party will reasonably assist the other party in remediating or mitigating any potential damage, including any notification which should be sent to individuals impacted or potentially impacted, or the provision of credit reporting services to such individuals. Each party shall bear the costs of such remediation or mitigation to the extent the breach or security incident was caused by it.

3. Mosaic Data Storage. Subject to the terms of this provision, Mosaic Data will be housed in a data center located in The United States or Canada. The Supplier represents and warrants that Mosaic Data shall not at any time during the term of the Agreement, be accessed, transmitted, or temporarily stored by the Supplier or its affiliates or subcontractors outside The United States and Canada. The Supplier shall encrypt in accordance with industry standards, or take other such reasonable security measures, to protect Mosaic Data in accordance with this Security Exhibit. the Supplier will (i) comply with applicable laws related to the security and processing of Mosaic Data, and (ii) will reasonably cooperate with Mosaic in its compliance with applicable law.

4. Logical Access Controls. Access to Mosaic Data by the Supplier and Supplier Parties in support of the services provided to Mosaic by the Supplier shall remain restricted on a "Need to Know" basis. When required, access will be granted based on the Least Privilege necessary to perform required business function on behalf of or in support of services provided by the Supplier. At no time shall Mosaic Data be accessible by or available to any third party except where explicit written consent is provided to the Supplier by Mosaic. The Supplier shall maintain logical access controls no less than industry standard for the nature of the services provided by the Supplier and appropriate for the legal requirements for the protection of Mosaic Data hosted, maintained, processed or otherwise accessed by the Supplier and Supplier Parties.

5. Physical Access Controls. Physical access controls shall be employed to restrict physical access to the hardware that accesses and or stores Mosaic Data to authorize the Supplier and the Supplier Party personnel who have a legitimate business need for such access. The Supplier shall maintain physical access controls in the same manner which it maintains physical access controls with regard to its own information, but in no event shall such physical access controls be less than industry standard for the nature of services provided by the Supplier to Mosaic.

6. Threat Management and Security Event Monitoring. The Supplier shall monitor security trends to maintain appropriate awareness of existing and emerging threats to the Confidentiality, Integrity and Availability of Mosaic Data. The Supplier shall incorporate information related to threats both current and emerging into the Security Program to actively manage and minimize the risk to Mosaic Data. The Supplier shall actively monitor the Supplier business computing environments for indicators of security events that could place the Confidentiality, Integrity or Availability of Mosaic Data at risk. Security event monitoring will operate in a manner that provides immediate notification of a data security breach, whether actual or potential.

7. Incident Response. The Supplier shall maintain an incident response program responsible for all Supplier computing resources that access, process, store, communicate or transmit Mosaic Data. The Supplier incident response program shall provide for a timely assessment and remediation of security events. The incident response program shall focus on minimizing the risk to Mosaic Data through the timely containment of security events, security event analysis and remediation planning, security event documentation and root cause analysis.

8. Information Protection. Only Authorized Supplier Employees using Supplier-supplied equipment may access Mosaic's computer network or systems. The Supplier shall use only Mosaic approved remote network access technology to access Mosaic's computer network or systems. Mosaic retains sole discretion on remote access technology and will provide the Supplier with thirty (30) days advance notice of changes to the remote access technology requirements. Prior to accessing Mosaic's computer network or systems, the Supplier shall ensure all Supplier Parties are aware of and are prepared to comply with Mosaic's Acceptable Use Policy and Code of Business Conduct and Ethics. While connected to or using Mosaic's computer network and systems, the Supplier shall not engage in any activity intended to disable or circumvent the security controls implemented by Mosaic. Mosaic Data used and/or created throughout the term of the Agreement by the Supplier shall remain with the Mosaic systems and network and shall not be stored on Supplier equipment or other non-Mosaic data storage devices unless otherwise explicitly agreed upon in writing prior to Mosaic Data leaving the Mosaic systems and/or network. The Supplier will promptly notify Mosaic whenever any of the Authorized Supplier Employees leave the Supplier's employ or no longer require access to Mosaic's computer network or systems. Additionally, the Supplier shall comply with the following requirements:

i. The Supplier must have policies and procedures in place to ensure that industry standard commercial anti-virus software is installed and kept up to date on all Supplier equipment that is used to access Mosaic network or systems;

ii. The Supplier must have policies and procedures in place to ensure that the latest security patches are applied in a timely manner to all Supplier equipment that is used to access Mosaic's network or systems;

iii. The Supplier must use an industry standard commercial email filtering and anti-virus application; and

iv. The Supplier must use an industry standard commercial web filtering software.

9. Definitions.

"Authorized Supplier Employees" is defined as those employees who are authorized to access Mosaic's computer network or systems. The Supplier shall provide to Mosaic a written list of the names, titles and location of the Supplier's employees that the Supplier is requesting should have access to Mosaic's computer network or systems. Mosaic shall have the opportunity to review and approve the listing of Authorized Supplier Employees. The Supplier shall be solely responsible for ensuring that Authorized Supplier Employees are not security risks.

"Confidentiality" is defined as maintaining controls over Mosaic Data in a manner that strictly enforces a "Need to Know" level of access. The "Need to Know" must be based upon a defined business need and include actions required to be performed by or on behalf of Mosaic directly related to Mosaic business processes or in direct support of the services provided by the Supplier to Mosaic.

"Integrity" is defined as the completeness and accuracy of Mosaic Data as entered, modified or updated in the Supplier environment.

"Availability" is defined as remaining available for use by Mosaic in the normal course of business, availability includes Mosaic Data, the associated storage devices, along with the associated hardware and software used to secure, access, or process Mosaic Data along with the associated communications channels managed by the Supplier in support of services provided to Mosaic.

"Least Privilege" is defined as providing the lowest level of access privileges (read, write, modify, delete, etc.) to Mosaic Data required in order to fulfill daily responsibilities necessary to act on behalf Mosaic or in support of services provided to Mosaic by the Supplier.