



004 Top 10 Things About Technology Law Every In-house Practitioner Should Know

Blake T. Bilstad

Senior Vice President, General Counsel & Secretary
Provide Commerce, Inc.

Gary A. Perlmutter

Senior Commercial Counsel
Sempra Energy

Joan B. Stafslie

Vice President & General Counsel, Clinical Technologies & Services
Cardinal Health, Inc.

Hillary M. Wilson

Senior Counsel - Clinical Technologies
Cardinal Health, Inc.

Faculty Biographies

Blake T. Bilstad

Blake T. Bilstad is the senior vice president, general counsel and secretary of Provide Commerce, Inc. an e-commerce company specializing in the delivery of flowers and other perishables direct from suppliers to consumers through its brands ProFlowers, Cherry Moon Farms, Uptown Prime and Secret Spoon. His responsibilities include managing all legal matters for the company including commercial contracts, mergers and acquisitions, intellectual property, privacy and internet law, corporate governance, securities, SEC and governmental compliance, litigation, insurance and real estate.

Prior to joining Provide Commerce, Mr. Bilstad worked with Vivendi Universal Net USA, the U.S. group of internet properties owned by Vivendi Universal S.A., a French-owned entertainment and telecommunications conglomerate, serving most recently as the group's senior vice president of legal affairs and secretary. He worked for MP3.com, Inc., a pioneering online music company that was acquired by Vivendi, and held a variety of legal positions there including vice president of corporate legal affairs, secretary and corporate counsel.

Prior to MP3.com, Mr. Bilstad was a business associate at the law firm of Cooley Godward LLP.

Mr. Bilstad holds a B.A., from Duke University and a J.D., cum laude, from Harvard Law School, where he was the Executive Editor of the Harvard Journal of Law & Technology and winner of the Irving Oberman Memorial Award writing prize.

Gary A. Perlmutter

Gary A. Perlmutter, senior commercial counsel at Sempra Energy in San Diego, is responsible for technology, Internet, and intellectual property legal matters, as well as credit and commercial finance matters. He counsels all of Sempra Energy's business units in these areas, including Sempra Global, a diversified energy services company with worldwide energy trading operations and electric generation, liquefied natural gas, pipeline, and other energy infrastructure facilities, and the Sempra utilities, Southern California Gas Company and San Diego Gas & Electric Company.

Prior to joining Sempra's legal department, Mr. Perlmutter practiced at Ervin, Cohen & Jessup in Beverly Hills and Procopio, Cory, Hargreaves and Savitch in San Diego as general business and corporate transactional attorney, with an emphasis on technology and banking matters.

Mr. Perlmutter received a B.A. from the University of California, Santa Cruz and is a graduate of the University of California-Hastings College of the Law.

Joan B. Stafslie

Joan B. Stafslie is vice president and general counsel for the clinical technologies and services (CTS) business segment of Cardinal Health, Inc. in San Diego. She is responsible for leading all legal activities for the CTS segment, including commercial matters, intellectual property, litigation, federal and state regulations, and international operations.

Prior to joining Cardinal Health, Ms. Stafslie was an associate with the law firm of Brobeck, Phleger & Harrison LLP in San Diego, specializing in real estate, general corporate, and environmental law. Prior to law school she worked as a chemical engineer and in sales for The Dow Chemical Company.

She currently serves on the Cardinal Health corporate diversity and inclusion steering council as well as leads the local San Diego diversity council. She also is actively involved with her church, including a Tijuana orphanage, which is supported by the church.

Joan earned her B.S. in chemical engineering from Northwestern University and a J.D. from University of Wisconsin Law School.

Hillary M. Wilson

Hillary M. Wilson is senior counsel for the clinical technologies and services business segment for Cardinal Health (CAH), a Fortune 20 global healthcare organization, located in San Diego. Her primary focus has been supporting the business in software development and licensing. She led the company's effort to develop an Open Source Code Policy and conducts training and discussion sessions with the different software development groups within her business segment.

Ms. Wilson was selected as the operational excellence deployment leader for the medication products business within clinical technologies and services. In that role, Ms. Wilson will establish, coordinate, and provide leadership for the design excellence - Lean Six Sigma initiatives, including developing research and development and marketing strategies, policies, objectives, plans, organizations, and procedures focused on integrating Lean Six Sigma methodologies in product development and design to cultivate a culture of design excellence. She has a passion for process improvement and has been a team member of several successful cross-functional operational improvement projects.

Ms. Wilson is a member of the board of directors for ACC's San Diego Chapter.

She earned her bachelor's degree from the University of California, Santa Cruz, and her law degree from Monterey College of Law.

LICENSE NAME	CATEGORY	COMPATIBLE w/ GPL?	DW's ¹ REQUIRED TO REMAIN OPEN?	INTEGRATION PROHIBITION?	DISTRIBUTION OF OBJECT CODE OR EXECUTABLE FORM?	UNIQUE FEATURES	RESTRICTIONS/ REQUIREMENTS
rg/copyleft/gpl.html			under GPL only)		one of the following: - provide complete source code, - provide 3yr offer to provide additional source code, or - provide the information licensee received as to the offer to distribute source code (provisions of source code must be under GPL license)	- Viral: all copies and modifications must be licensed under GPL - licensees cannot add additional restrictions on licenses for modified work	LICENSEE must: - Conspicuously publish (1) CR notice and (2) warranty disclaimer - Keep all notices referencing the GPL and the absence of warranty intact - Provide copy of GPL Modifications: To distribute DWs licensee must: - Provide prominent notices of modification - License whole work under GPL (i.e. must make source code of DW open) - Interactive works must display CR notice, warranty disclaimer and copy of GPL
GNU LGPL http://www.gnu.org	Restrictive Hybrid	Yes	Yes (and may be licensed	Can be linked to non (L)GPL	OK under terms of	DW's can be licensed under	Copies: To distribute copies

LICENSE NAME	CATEGORY	COMPATIBLE w/ GPL?	DW's ¹ REQUIRED TO REMAIN OPEN?	INTEGRATION PROHIBITION?	DISTRIBUTION OF OBJECT CODE OR EXECUTABLE FORM?	UNIQUE FEATURES	RESTRICTIONS/ REQUIREMENTS
Apache License Version 2.0 http://www.apache.org/licenses/LICENSE-2.0.html	Permissive	Likely/ Not (b/c allows licensee to provide additional or different license terms)	No	No	No restrictions	licensee's modifications may provide additional or different license terms and conditions for use provided licensee's use otherwise complies with License	To reproduce and distribute copies of DWs LICENSEE must: - Provide copy of License - Provide notice of modified files stating they have been changed from original - Retain all CR ² , patent, trademark, and attribution notices
BSD http://www.open source.org/licenses/bsd-license.php	Permissive	Yes	No	No	No restrictions	Arguably one of the most permissive Licenses	Redistributors must retain CR notice, a list of the License's conditions, and a disclaimer No Endorsement: No use of UCB's name or contributors' names for endorsement/pr omotion
GNU GPL http://www.gnu.org	Restrictive		Yes (and must be licensed	Yes	OK provided licensee does	- First OSL - Most Restrictive	Copies: To distribute copies

¹ Derivative Work
² Copyright

LICENSE NAME	CATEGORY	COMPATIBLE w/ GPL?	DWS ¹ REQUIRED TO REMAIN OPEN?	INTEGRATION PROHIBITION?	DISTRIBUTION OF OBJECT CODE OR EXECUTABLE FORM?	UNIQUE FEATURES	RESTRICTIONS/ REQUIREMENTS
ses/mit-license.php							- Include CR notice and permission notice in copy or DW distribution.
Mozilla Public License http://www.mozilla.org/MPL/MPL-1.1.html	Restrictive Hybrid	No	Yes (code copied or modified must stay under MPL)	No (may be combined with proprietary files)	Ok but must make source code available under terms of License on same media as executable version or via an accepted Electronic Distribution Mechanism (must remain available for at least 12 months)	-Requires inclusion of a Legal.txt file describing third party intellectual property claims to covered/original work	- Include CR notice and permission notice in copy or DW distribution. - Copies: To distribute copies of work license must: - distribute under MPL only - include copy of MPL - not offer or impose new License terms but may offer additional rights) - duplicate the notice in MPL's exhibit A in each file of the source code Modifications: To distribute modifications of work license must: - distribute under MPL only - include file stating origin of work, that work has been changed and documenting changes made - include

LICENSE NAME	CATEGORY	COMPATIBLE w/ GPL?	DWS ¹ REQUIRED TO REMAIN OPEN?	INTEGRATION PROHIBITION?	DISTRIBUTION OF OBJECT CODE OR EXECUTABLE FORM?	UNIQUE FEATURES	RESTRICTIONS/ REQUIREMENTS
rg/copy/et/lesse.html							licensee must: - Conspicuously publish (1) CR notice and (2) warranty disclaimer - Keep all notices referencing the LGPL and the absence of warranty intact - Provide copy of LGPL Modifications: To distribute DWS licensee must: - Provide prominent notices of modification - License whole work under LGPL or GPL (i.e. must make source code of DW open) - Interactive works must display CR notice, warranty disclaimer and copy of LGPL
MIT Expat License http://www.open source.org/licenses.html	BSD-Style Permissive	Yes	No	No	No restrictions	Just like BSD except no Non-endorsement clause	To copy, modify, and distribute work licensee must:
							under LGPL or GPL Note: software which merely link to LGPL'd software do not have to be (L)GPL'd just DWS
							software (which may be free or proprietary)
							License if licensee provides complete source code and releases object code under same terms in Section 1 and 2 of License. If distribution of object code is made by offering access to copy from a designated place then offering equivalent access to source code is ok.

LICENSE NAME	CATEGORY	COMPATIBLE w/ GPL?	DWS ¹ REQUIRED TO REMAIN OPEN?	INTEGRATION PROHIBITION?	DISTRIBUTION OF OBJECT CODE OR EXECUTABLE FORM?	UNIQUE FEATURES	RESTRICTIONS/ REQUIREMENTS
							Legal.txt file describing all known third party rights re: work - duplicate the notice in MPL's exhibit A in each file of the source code

SAMPLE HIPAA PRIVACY POLICY

1.0 PURPOSE

- 1.1 The purpose of this document is to ensure that corporate privacy policies and procedures are current and up to date with current legal and regulatory requirements and to set forth record retention guidelines for documents designated under HIPAA.

2.0 DEFINITIONS

Unless a specific policy indicates otherwise, any defined term has the meaning ascribed to it in this Glossary.

- 2.1 **Access** - The ability or the means necessary to read, write, modify or communicate data/information or otherwise use any system resource.
- 2.2 **Administrative Safeguards** - Administrative actions, and policies and procedures, to manage the selection, development, implementation and maintenance of security measures to protect electronic protected health information and to manage the conduct of Company's workforce in relation to the protection of that information.
- 2.3 **Authentication** - The corroboration that a person is the one claimed.
- 2.4 **Availability** - The property that data or information is accessible and useable upon demand by an authorized person.
- 2.5 **Business Unit** - Any one or more business units, departments or divisions of Company.
- 2.6 **Chief Information Officer or CIO** - That individual responsible for the Company's IT department.
- 2.7 **Company IT** - The department of Company responsible for implementing, maintaining and managing Company's information systems.
- 2.8 **Confidentiality** - The property, data or information that is not made available or disclosed to unauthorized persons or processes.
- 2.9 **De-identification (Statistical Methods)** - Accepted statistical and scientific principles and methods for rendering information not individually identifiable.
- 2.10 **De-identification (Safe Harbor)** - The eighteen (18) specific identifiers of the individual or relatives, employers or household members of the individual are removed from the electronic PHI.
- 2.11 **Electronic Media:**
 - 2.11.1 Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or
 - 2.11.2 Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet (using Internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media; provided, however, that certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be

- transmissions via electronic media under the Security Rule, because the information being exchanged did not exist in electronic form before the transmission.
- 2.12 EISA or the Electronic Information Security Administrator** for the respective Business Unit.
- 2.12.1 Information Security Coordinator** – The individual tasked by the Company's management to have oversight responsibility for the development, implementation, and operation of the company's privacy compliance program.
- 2.12.2 Electronic Information Security Administrator** – The individual responsible for the development and implementation of the Company's Business Unit's HIPAA security rule policies and procedures.
- 2.13 Electronic Protected Health Information (EPHI)** – The subset of Individually Identifiable Health Information that is (i) transmitted by electronic media; or (ii) maintained in any medium constituting electronic media; provided, however, that EPHI does not include such information included in certain education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. §1232g, or employment records held by Company in its role as employer.
- 2.14 Encryption** – The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.
- 2.15 Enterprise IT Service Center** – That department of Company IT responsible for handling user questions, comments, or problems (commonly referred to as a "help desk").
- 2.16 Facility** – The physical premises and the interior and exterior of a building(s).
- 2.17 Global Security** – That department of the Company responsible for the physical security of Company, including its premises, buildings and equipment.
- 2.18 HIPAA** – The Health Insurance Portability and Accountability Act of 1996, as it may be amended from time to time, and all rules and regulations promulgated thereunder.
- 2.19 Individually Identifiable Health Information** – Information that is a subset of health information, including demographic information collected from an individual, and (a) is created or received by a health care provider, health plan, or health care clearinghouse; and (b) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (i) identifies the individual, or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
- 2.20 Information System (IS or Information Technology (IT))** – An interconnected set of information resources under the same direct management control that shares common functionality. An information system normally includes hardware, software, information, data, applications, communications and people.
- 2.21 Integrity** – The property that data or information have not been altered or destroyed in an unauthorized manner.
- 2.22 IPT or Company Health IPT** – Company Health Information Protection Team.
- 2.23 Malicious Software** – Software designed to damage or disrupt a system (e.g., a virus).
- 2.24 Password** – Confidential authentication information composed of a string of characters.
- 2.25 Physical Safeguards** – Physical measures, policies and procedures (e.g., locks and identification cards) to protect Company's electronic information systems and related buildings and equipment, from natural and environmental hazards and from unauthorized intrusion.
- 2.26 President of Business Unit** – The individual who is responsible for the applicable Business Unit.
- 2.27 Protected Health Information (PHI)** – Health information, including demographic information collected from an individual, that: (i) is created or received by the Company; (ii) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and, (iii) identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. This includes information in any media including electronic, written and verbal.
- 2.28 Security or Security Measures** – All of the administrative, physical, and technical safeguards in an information system.
- 2.29 Security Incident** – The attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system.
- 2.30 Security Rule** – The Security Standards for the Protection of Electronic Protected Health Information, 45 C.F.R. Part 164, promulgated pursuant to HIPAA, as it may be amended from time to time.
- 2.31 Security Rule Policy** – The Business Unit's HIPAA Security Rule policies and procedures described herein.
- 2.32 Technical Safeguards** – The technology and the policy and procedures for its use that protect electronic protected health information and control access to it.
- 2.33 User** – A person or entity with authorized access.
- 2.34 Workstation** – An electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.
- 3.0 RESPONSIBILITIES**
- 3.1 Every employee of the Company** who may have access to PHI must understand the purpose and scope of HIPAA. In addition, those employees who have access to PHI as defined under 45 CFR Part 164.501 and in Section 4.8 of the Quality Procedure are responsible for complying with the requirements under this HIPAA Policy.
- 3.2 Contracts Administration, Customer Advocacy, Law Department, Professional Services, Technical & Field Services, Sales, Marketing, and Research & Development** are responsible for:

- 3.2.1** Properly managing PHI received from Covered Entities.
- 3.2.2** Confirming that the Company is authorized to access, collect, retain, user, disclose and, if applicable, to de-identify the PHI. (See 45 CFR Part 164.502 – Part 164.5[
- 3.2.3** If access to PHI is authorized under a Business Associate contract (see 45 CFR Part 164.504(e).) ensuring that the PHI is (a) properly de-identified where appropriate by stripping the Individually Identifiable Health Information of identifying facts and/or (b) disclosed only as authorized by the Covered Entity and only as minimally necessary to perform authorized services as described in the Sales Agreement and/or Business Associate contract with the Covered Entity.
- 3.2.4** Upon termination of a relationship with Covered Entity, either returning the PHI to the Covered Entity, if feasible, or certifying in writing to Covered Entity that appropriate safeguards protecting the PHI will continue in accordance with HIPAA and the Business Associate contract with the Covered Entity. (See 45 CFR Part 164.504(e)(2)(ii)(I).)
- 3.2.5** Ensuring that any agent, including a consultant or contractor whom the Company engages and who has access to PHI, agrees in writing to the same restrictions and conditions that apply to Company under HIPAA and under any applicable Business Associate contract with the Covered Entity. (See 45 CFR Part 164.504(e)(2)(ii)(D).)
- 3.2.6** If, after review and approval of the Business Associate contract or other associated agreement, the Law Department notifies Contracts Administration of a non-standard restriction on access to PHI, Contracts Administration will enter this information in the Customer file or the Customer Relations Management System (“CRM System”) indicating that access to such data is not authorized without first consulting with the Law Department. All employees who may have a need to access PHI are required to check with Contracts Administration or the CRM System prior to accessing the PHI in order to confirm that non-standard restrictions do not apply to that particular customer account.
- 3.3** **Contract Administration** is responsible for:
- 3.3.1** Circulating to the Law Department for comment and monitoring execution of Business Associate contracts.
- 3.3.2** After review and approval by the Law Department, confirming that the Business Associate contract is properly executed by authorized individuals.
- 3.3.3** Maintaining in its contract files the executed Business Associate contracts.
- 3.3.4** Tracking whether such Business Associate contracts have terminated along with any underlying agreements and notifying the Law Department of such termination.
- 3.3.5** If, after review and approval of the Business Associate contract, the Law Department has identified a non-standard restriction on access to PHI or De-identified Information, Contract Administration will note such restriction in the Customer file or the CRM System.
- 3.3.6** Confirming whether a particular Customer has agreed in writing to allow Company to aggregate, de-identify, and use Customer’s data.
- 3.4** **Law Department** is responsible for:
- 3.4.1** Reviewing Business Associate contracts or other agreements with Covered Entities that may restrict or affect the use or treatment of Individually Identifiable Health Information, including any agreements with consultants or other third parties for HIPAA compliance.
- 3.4.2** Assisting other departments within the Company in determining the Company’s legal obligations in gathering, protecting using, disclosing, returning, and destroying PHI.
- 3.4.3** Notifying Contracts Administration of a Covered Entity’s non-standard restrictions on access to PHI or De-identified Information.
- 3.4.4** Notifying Covered Entities of unauthorized disclosures of PHI by the Company pursuant to 45 CFR Part 164.504(e)(2)(ii)© and developing procedures to mitigate, to the extent practicable, any harmful effects of unauthorized disclosures.
- 3.4.5** Responding to Covered Entities or patient requests to: (1) provide access to PHI in the possession of Company; (2) make amendments to PHI in the possession of the Company; (3) provide an accounting of disclosures of PHI made by the Company, and (4) make available to the Covered Entity or to the Secretary of the United States Department of Health and Human Services the internal practices, books, or records of the Company relating to the Company’s use and disclosure of PHI in order to confirm the Covered Entity’s compliance with HIPAA. (See 45 CFR Part 164.504(e)(2)(ii)(E) – (H).)
- 3.4.6** Responding to any requests for disclosure of PHI required pursuant to a subpoena or other legal process. (See 45 CFR Part 164.504(e)(4)(II).)
- 3.5** **Regulatory** is responsible for:
- 3.5.1** Reviewing current HIPAA regulations so that any HIPAA impact is given necessary consideration to products as they are submitted through the regulatory process.
- 3.5.2** Assessing compliance to this procedure as part of the regular scheduled internal quality audits of the Company facilities.
- 3.6** **Customer Advocacy** is responsible for:
- 3.6.1** Responding to customer complaints and regulatory issues involving a device that may contain PHI.
- 3.6.2** Responding to any requests for disclosure of PHI required pursuant to a subpoena, governmental requirement, or other legal process. (See 45 CFR Part 164.504(e)(4)(ii).)
- 3.7** **Information Technology** is responsible for:
- 3.7.1** Understanding the HIPAA Security Standards as set forth in 45 CFR Part 164.302 – Part 164.318 that became effective on April 20, 2005.
- 3.7.2** Implementing administrative, physical, and technical safeguards that reasonable and appropriately protect the integrity, confidentiality, and

availability of electronic PHI that the Company creates, receives, maintains, or transmits on behalf of a Covered Entity.

- 3.7.3** Protecting against reasonable anticipated threats or hazards to the security or integrity of the electronic PHI and implementing policies and procedures to prevent, detect, contain, and correct security violations.
- 3.7.4** Ensuring that any agent or subcontractor to whom the Company provides such electronic PHI agrees to implement reasonable and appropriate security safeguards to protect it.
- 3.7.5** Reporting to the Covered Entity any security incident of which the Company becomes aware.

4.0 REQUIREMENTS

4.1 Accounting of Non-Routine Disclosures of Protected Health Information:

- 4.1.1** It is the policy of the Company to provide customers, upon request, an accounting of certain disclosures of Protected Health Information (PHI) made by the Company or by a subcontractor of the Company which has or has used PHI.

4.2 Amendment of Protected Health Information:

- 4.2.1** It is the policy of the Company to respond to customers' requests that the Company amend protected health information (PHI) or a record about a patient in a designated record set for as long as the protected health information is maintained in the designated record set. For purposes of this policy, a "designated record set" means records, i.e., any item, collection or grouping of information, maintained by the Company that includes:
- A. the medical records and billing records of individuals,
 - B. enrollment, payment, claims adjudication, case or medical management records;
 - C. records used, in whole or in part, by or for the Company or a healthcare provider (that employs the Company as a business associate) to make decisions about individuals.

4.3 Commitment to Privacy, Use/Disclosure of Minimum Necessary Information, and Verification of Identity:

- 4.3.1** The Company is committed to protecting the privacy of PHI received from our customers. The Company will not use or disclose PHI received from our customers except as authorized by agreements with our customers or as required by law. Company employees that receive, handle, or use PHI are required to review or use the PHI only to the extent that it is minimally necessary to perform duties for the Company. Prior to disclosing any PHI to a third party, Company employees shall determine that disclosure is appropriate and shall verify the identity and authority of the third party.

4.4 Contracting with Subcontractors:

- 4.4.1** It is the policy of the Company to contract with subcontractors who respect patient privacy. Company subcontractors that use PHI received from the Company shall be subject to the same terms and conditions with regard to the

PHI as binds the Company in the business associate agreement with the customer (the "**Business Associate Agreement**"). It is further the policy of the Company to investigate any information it receives indicating that a subcontractor may have breached its obligations relating to PHI and to take appropriate steps, as outlined in this policy, where such breaches have occurred.

4.5 Business Associate Agreements:

- 4.5.1** It is the policy of the Company to protect the right of privacy of all of its customer's patients. It is further the policy of the Company that whenever it is acting as a Business Associate in accordance with the Health Insurance Portability and Accountability Act and regulations promulgated pursuant thereto ("HIPAA"), to enter into a Business Associate Agreement with that customer.

4.6 Customer Requests for Access to Protected Health Information:

- 4.6.1** It is the policy of the Company to respond to a customer's requests for Protected Health Information in a timely manner consistent with the provisions of the customer's business associate contract as long as the protected health information is maintained in the designated record set. For purposes of this policy, a "designated record set" means records, i.e., any item, collection or grouping of information, maintained by the Company that includes:
- A. the medical records and billing records of individuals,
 - B. enrollment, payment, claims adjudication, case or medical management records;
 - B. records used, in whole or in part, by or for the Company or a healthcare provider (that employs the Company as a business associate) to make decisions about individuals.

4.7 Use and Disclosures of De-identified Information:

- 4.7.1** It is the policy of the Company to protect the PHI received from the Company's customer or their agents. The Company may use and disclose de-identified health information. De-identified health information is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. Health information shall be considered de-identified only if either of the approved de-identification procedures, Statistical Methods or Safe Harbor, are followed.
- 4.7.2** Company may use health information received from Company customers to create de-identified health information in accordance with this Policy.

4.8 Government Investigations – Privacy-Related Matters:

- 4.8.1** It is the Company's practice to cooperate with government investigations in the most accurate and truthful manner possible. In order to ensure that such cooperation occurs in an organized and accurate manner, the Company has developed this policy to assist employees in responding to government requests for information relating to privacy related issues or matters.

- 4.9 Internal Enforcement:**
- 4.9.1** The Company has adopted this discipline policy to address employee violations of federal and state privacy laws and/or the Company's privacy policies ("Privacy Violations"). The Human Resources Director and the employee's immediate supervisor, in consultation with the **Information Security Coordinator (or Privacy Official)**, will administer appropriate discipline related to Privacy Violations, consistent with the procedures established below.
- 4.9.2** Management retains full discretion with respect to any discipline for violation of the PHI policy. Discipline can include one or more of the following: informal counseling, verbal warning, written warning, probation, suspension, demotion or termination. Factors such as the nature and duration of the offense, severity and frequency will be considered. Additionally, restitution may be required, where appropriate.
- 4.10 Non-Routine Disclosures of Protected Health Information:**
- 4.10.1** It is the policy of the Company to protect the privacy of Protected Health Information received from the Company's customers or their agents. The Company routinely uses and discloses Protected Health Information provided to the Company by its customers so as to provide healthcare-related support services. In the event that the Company receives a request for a disclosure of Protected Health Information for any other purpose ("**Non-routine Disclosure**"), it is the Company's policy to handle such request in accordance with the Business Associate Agreements between the Company and its customer subject to applicable law.
- 4.11 Reporting Unauthorized Disclosures:**
- 4.11.1** It is the policy of the Company to protect the PHI received by the Company in compliance with the relevant terms of the Company's Business Associate Agreements and the Company's policies and procedures created in connection with the HIPAA Privacy Requirements ("HIPAA Policies"). It is the policy of the Company to advise the Company's customers in a timely manner in the event of a disclosure in violation of the Company's Business Associate Agreements. The Company has set forth a process for employees and other individuals to alert the Company to potential Unauthorized Disclosures. It is also the policy of the Company, upon receiving notice of a potential Unauthorized Disclosure, to make a determination whether an Unauthorized Disclosure occurred and if an Unauthorized Disclosure did occur, to notify the customer of the Unauthorized Disclosure.
- 4.12 Safeguarding Patient Information:**
- 4.12.1** It is the policy of the Company to safeguard the privacy of the Protected Health Information (PHI) received by the Company's customers. As a result, the Company has adopted administrative, technical and physical safeguards to protect the privacy of PHI.
- 4.13 Termination of Customer Relationships:**
- 4.13.1** [Implementation Note: When a customer relationship terminates, a Business Associate must either return or destroy the information, or must determine that return or destruction is not feasible and protect the information on an ongoing basis. There are optional approaches for the policy that the Company will adopt depending on its own business considerations and depending on the content of its Business Associate contracts. The Company could determine that it will always return the information, that it will always destroy the information or that it will never be feasible to return or destroy the information and set forth appropriate procedures in this policy. In the alternative, The Company could use this Policy to set forth a number of factors to guide the Information Security Coordinator (or Privacy Official) in making this determination on a case by case basis. In its current form, this Policy is drafted to allow the Information Security Coordinator (or Privacy Official) to make this determination on a case by case basis, but can be modified to reflect one of the other approaches, if desired.]
- 4.13.2** The Company is committed to safeguarding the Protected Health Information received by its customers. As a result, when a customer relationship is terminated, the Company will make a determination whether it is feasible to return or destroy such Protected Health Information and if it is feasible will act to return or destroy the information in a thorough and prompt manner. In the event that the Company determines that it is not feasible to return or destroy the Protected Health Information, it is the Company's policy to continue to protect such information on an ongoing basis after the termination of the customer contract.
- 4.14 Workforce Training:**
- 4.14.1** It is the policy of the Company to provide training to all applicable Company employees on the Company's privacy policies as necessary and appropriate for the employees to carry out their specific job duties at the Company.
- 4.15 Use and Disclosure of Limited Data Set (including Data Use Agreement):**
- 4.15.1** It is the policy of the Company to protect the PHI received from the Company's customer or their agents. The Company may use and disclose a limited data set (LDS). A LDS is a set of records where several specified direct patient identifiers have been removed, but the records have not been completely de-identified. Conversely, de-identified health information is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. In the event de-identified information is to be created or used, Company employees or subcontractors should refer to the Company "Use and Disclosures of De-Identified Information" policy. Health information shall be considered to be a LDS only if the procedures to create or use a LDS are followed.
- 4.15.2** The Company may create, use or disclose a LDS only for the purposes of research, public health, or health care operations, so long as the Company and its customer, who is a Covered Entity (e.g., healthcare provider, health plan or healthcare clearing house), enter into a data use agreement.
- 4.16 Non-Retaliation Action:**

4.16.1 The Company is committed to safeguarding Protected Health Information (PHI) received from its customers and ensuring that this information is protected against inappropriate use or misuse. To ensure that this is accomplished, it is the policy of the Company that no retaliatory action(s) are taken against any individual or employee who in good faith reports any suspected unlawful actions involving PHI to the appropriate individuals within the Company or the appropriate government authorities which includes the U.S. Department of Health and Human Services Office of Civil Rights.

4.17 Privacy Policy Updates and Record Retention:

4.17.1 The Company is committed to maintaining privacy policies and procedures that meet current legal and regulatory requirements and to ensuring that privacy-related documents are maintained as required by law.

4.18 Information Security Coordinator:

4.18.1 The Company is committed to safeguarding the Protected Health Information received from its customers. As a result, the position of Information Security Coordinator has been created within the Company to ensure that this is accomplished.

5.0 PROCEDURE – Not Used

6.0 REFERENCE DOCUMENTS – Not Used

The following reference documents are applicable to this document.

SAP Document	Title
N/A	N/A

7.0 APPENDIX – Not Used

SAMPLE HIPAA SECURITY POLICY

1.0 PURPOSE

1.1 The purpose of this document is to provide a uniform method of complying with the Security Rule, where applicable to designated business units that are covered entities and protecting EPHI of customers from accidental or deliberate disclosure, misuse, unauthorized access or unavailability. In addition, this Security Rule Policy is intended to raise the level of awareness of all of the Company's workforce of the need for attention to matters related to the access, handling and destruction of EPHI. It is the expectation of the Company that each member of the workforce who comes in contact with PHI will review and comply with this Security Rule Policy.

1.2 This Security Rule Policy is designed to complement, supplement and be implemented in conjunction with the Company's Information Protection Policy and Company's general security rules, policies and procedures. This Security Rule Policy is not, and should not be considered, a comprehensive replacement of such Information Protection Policy, Facility Security and Access Procedures and/or other general security rules, policies and procedures of Company, but rather applies to the protection and security of EPHI.

2.0 DEFINITIONS

Please refer to QSP2100 Privacy Policy - Health Insurance Portability and Accountability Act (HIPAA) for a list of definitions.

3.0 RESPONSIBILITIES

Please refer to QSP2100 Privacy Policy - Health Insurance Portability and Accountability Act (HIPAA) for a list of responsibilities.

4.0 REQUIREMENTS

4.1 Administrative Safeguards:

4.1.1 Standard: Implement policies and procedures to prevent, detect, contain, and correct security violations. Implementation specifications for this standard are as follows:

4.1.1.1 Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic Provided Health Information (EPHI).

4.1.1.2 Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the Security Rule.

4.1.1.3 Apply appropriate sanctions against workforce members who fail to comply with the Company's Security Rule Policy.

4.1.1.4 Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

- 4.1.2** Standard: Identify the EISA (Electronic Information Security Administrator) who is responsible for the development and implementation of the policies and procedures required by the Security Rule.
- 4.1.3** Standard: Implement policies and procedures to ensure that all members of Company's workforce have appropriate access to EPHI, as provided under this Security Policy, and to prevent those workforce members who do not have such access from obtaining access to EPHI. Implementation specifications for this standard are as follows:
- 4.1.3.1** Implement procedures for the authorization and/or supervision of workforce members who work with EPHI or in locations where it might be accessed.
- 4.1.3.2** Implement procedures to determine that the access of a workforce member to EPHI is appropriate.
- 4.1.3.3** Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made with respect to security clearance procedures under this Security Policy.
- 4.1.4** Standard: Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of the HIPAA security rule. Implementation specifications for this standard are as follows:
- 4.1.4.1** Implement policies and procedures for granting access to EPHI, for example, through access to a workstation, transaction, program, process, or other mechanism.
- 4.1.4.2** Implement policies and procedures that, based upon Company's access authorization policies, establish, document, review and modify a user's right of access to a workstation, transaction, program or process.
- 4.1.5** Standard: Implement a security awareness and training program for all members of Company workforce (including management) in those business units using, storing, or creating EPHI, or who have access to PHI. Implementation specifications for this standard are as follows:
- 4.1.5.1** Implement periodic security updates.
- 4.1.5.2** Implement procedures for guarding against, detecting, and reporting malicious software.
- 4.1.5.3** Implement procedures for monitoring log-in attempts and reporting discrepancies.
- 4.1.5.4** Implement procedures for creating, changing and safeguarding passwords.
- 4.1.6** Standard: Implement policies and procedures to address security incidents. Implementation specifications for this standard are as follows:
- 4.1.6.1** Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to Company and document security incidents and their outcomes.
- 4.1.7** Standard: Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence that damages systems that contain EPHI. Implementation specifications for this standard are as follows:
- 4.1.7.1** Establish and implement procedures to create and maintain retrievable exact copies of EPHI.
- 4.1.7.2** Establish (and implement as needed) procedures to restore any loss of data.
- 4.1.7.3** Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of EPHI while operating in emergency mode.
- 4.1.7.4** Implement procedures for periodic testing and revision of contingency plans.
- 4.1.7.5** Assess the relative criticality of specific applications and data in support of other contingency plan components.
- 4.1.8** Standard: Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under the HIPAA Security Rule and subsequently, in response to environmental or operational changes affecting the security of EPHI, that establishes the extent to which Company's security policies and procedures meet the requirements of the HIPAA Security Rule.
- 4.1.9** Standard: Company may permit a business associate or subcontractor to create, receive, maintain, or transmit EPHI on the Company's behalf only if Company obtains satisfactory assurances, in accordance with this Security Policy, that the business associate or subcontractor will appropriately safeguard the information. (This standard does not apply with respect to the transmission by Company of EPHI to a health care provider concerning the treatment of an individual.) Implementation specifications for this standard are as follows:
- 4.1.9.1** Document the required satisfactory assurances through a written contract or other arrangement with the business associate/subcontractor that meets the requirements of this policy and, if applicable, Company policies adopted pursuant to the HIPAA Privacy Rule.
- 4.2** **Physical Safeguards:**
- 4.2.1** Standard: Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. Implementation specifications for this standard are as follows:
- 4.2.1.1** Establish and implement procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

- 4.2.1.2 Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
- 4.2.1.3 Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
- 4.2.1.4 Implement policies and procedures to document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors and locks).
- 4.2.2 Standard: Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access EPHI.
- 4.2.3 Standard: Implement physical safeguards for all workstations that access EPHI to restrict access to authorized users.
- 4.2.4 Standard: Implement policies and procedures that govern the receipt and removal of hardware the electronic media that contain EPHI into and out of a Facility, and the movement of these items within the Facility. Implementation specifications for this standard are as follows:
 - 4.2.4.1 Implement policies and procedures to address the final disposition of EPHI and/or the hardware or electronic media on which it is stored.
 - 4.2.4.2 Implement procedures for removal of EPHI from electronic media before the media are made available for re-use.
 - 4.2.4.3 Maintain a record of the movements of hardware and electronic media and any person responsible therefore.
 - 4.2.4.4 Create a retrievable, exact copy of EPHI, when needed, before movement of equipment.
- 4.3 **Technical Safeguards:**
 - 4.3.1 Standard: Implement technical policies and procedures for electronic information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights pursuant to this Security Rule Policy. Implementation specifications for this standard are as follows:
 - 4.3.1.1 Assign a unique name and/or number for identifying and tracking user identity.
 - 4.3.1.2 Establish and implement procedures for obtaining necessary EPHI during an emergency.
 - 4.3.1.3 Implement electronic procedures that locks an electronic session after a predetermined time of inactivity. The user is then required to enter their network logon credentials to reactivate the session.
 - 4.3.1.4 Implement a mechanism to encrypt and decrypt EPHI.
 - 4.3.2 Standard: Implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI.

- 4.3.3 Standard: Implement policies and procedures to protect EPHI from improper alteration or destruction. Implementation specifications for this standard are as follows:
 - 4.3.3.1 Implement electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner.
- 4.3.4 Standard: Implement procedures to verify that a person or entity seeking access to EPHI is the one claimed.
- 4.3.5 Standard: Implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network. Implementation specifications for this standard are as follows:
 - 4.3.5.1 Implement security measures to ensure that electronically transmitted EPHI is not improperly modified without detection until disposed of.
 - 4.3.5.2 Implement a mechanism to encrypt EPHI whenever deemed appropriate.
- 4.3.6 Standard: Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the Security Rule. Amend policies and procedures, and document accordingly.

5.0 PROCEDURE – Not Used

6.0 REFERENCE DOCUMENTS

The following reference documents are applicable to this document.

SAP Document	Title
10000021409	QSP2100 Health Insurance Portability and Accountability Act (HIPAA) Privacy Policy

7.0 APPENDIX – Not Used

[SAMPLE]

PATENT MANUAL
ACME TECHNOLOGY, CO.

PATENT MANUAL
ACME TECHNOLOGY, CO.
TABLE OF CONTENTS

- I. INTRODUCTION.....
- II. WHAT IS PATENTABLE?.....
- III. WHERE CAN PATENTS BE OBTAINED AND HOW ARE PATENTS MAINTAINED?.....
- IV. WHO IS AN INVENTOR?.....
- V. PREPARATION OF THE PATENT APPLICATION
- VI. ACME PATENT COMMITTEE
- VII. WHICH INVENTIONS WILL ACME PATENT?.....
- VIII. WHICH INVENTIONS WILL BE FILED INTERNATIONALLY?
- IX. PROCESS FOR PATENT FILINGS
- X. LIMITATIONS ON PUBLIC DISCLOSURE
- XI. ACME INVENTOR RECOGNITION PROGRAM
- XII. PROTECTING PATENT RIGHTS OFACME:
- XIII. MAINTAINING LABORATORY NOTEBOOKS
- XIV. INVENTION DISCLOSURES.....
- XV. AVOIDING PATENT INFRINGEMENT
- XVI. PUBLICLY AVAILABLE SOURCES OF INFORMATION
- XVII. FURTHER QUESTIONS

PATENT MANUAL

ACME TECHNOLOGY, CO.

I. INTRODUCTION

Intellectual property, or as it is more commonly known, "IP", is as important an asset to a company as its products.

Without the protection that IP provides, competitors will soon copy a successful product. Because IP-copying competitors do not need to make the research and development investment into the product, nor spend the time and resources to make a product "manufacturable," nor develop a market for the product, it is likely that their costs, and consequently, their prices will be lower than the developer. Fortunately, the law in the United States and most advanced countries recognize this fact and have decided to encourage inventors and developers, while inhibiting IP thieves, copiers and followers.

Patents are a part of IP. Other valuable IP assets are trademarks, copyrights and trade secrets, but the focus here is on patents. Patents simply provide the patent owner the right to exclude competitors from practicing the patented invention for a period of time, generally twenty years from the filing date of the patent application. Here is another way to think about patents: Patents are like the deed to a piece of land by which the owner can exclude trespassers. To compete with the patentee, competitors must either wait for the patent to expire or invest time and financial resources to design around the patented invention, which in many cases, is no easy task.

Obtaining patents not only helps the Acme Technology, Co. ("Acme") business by protecting its products, it provides public recognition for the contributions of the inventors. We invest large sums in researching, prosecuting and protecting our patent assets and we have more than XXX United States and counterpart patents in numerous countries around the world. This manual is intended to provide guidance to assist you in establishing patent protection for the innovative developments resulting from the efforts of the many highly creative people at Acme.

It is a longstanding policy of Acme to respect the intellectual property rights of others.

II. WHAT IS PATENTABLE?

In general, any invention that is novel and non-obvious over what was done before is patentable.

The following categories exist in the U.S. patent law: processes, machines, manufactures, compositions of matter, or any new and useful improvements. Computer programs, electronic circuits, electronic devices, methods of doing business, methods of processing data, materials, drugs, living organisms, and mechanical devices are all patentable. However, in many countries of the world, including Europe, methods or processes of diagnosing and treating humans are not patentable, although the equipment used in diagnosing and treating humans is patentable.

There is a third requirement for an invention to be patentable. Not only must an invention be novel and non-obvious over what was done before, but it must also be useful. Although the words may be different in the various patent systems, these three requirements are generally applied throughout the world. For example, in Europe, an invention must be "novel", have "industrial applicability" (useful), and include an "inventive step" (non-obvious) over what was done before.

"Useful" or "industrial applicability" requires that the invention can be practiced, among other things. Because perpetual motion machines contravene the laws of physics and cannot be practiced, they are not "useful" and patents are not permitted for them. In the event that the inventor is not sure if his or her invention is "non-obvious" or includes an "inventive step", it is better to disclose the invention to the Acme Legal Department. A "novelty search" can be conducted to investigate the work previously done by others in the field so that an informed decision on patentability can be made.

Two main types of patents are available: utility patents and design patents. "Utility" patents cover functional features while "design" patents cover ornamental features. For example, the operational features of a novel and non-obvious product would be protected by a utility patent or patents while the overall ornamental "look" of the outside of the product could be protected by a design patent. As an example, Exhibit A presents a design patent on the ornamental features of the XXXX product, while Exhibit B presents a utility patent on the XXX design of the YYYY product.

The term in most countries of the world of a utility patent is twenty years from the filing date of the patent application. The term in many countries of a design patent is fourteen years from its issue date, although it is much longer in some countries.

III. WHERE CAN PATENTS BE OBTAINED AND HOW ARE PATENTS MAINTAINED?

A patent may be obtained in almost every country of the world. However, in most countries, it is quite expensive to obtain and maintain a patent. Most countries have an examination system and this involves further expense in obtaining a patent. Patent examiners typically have one or more reservations about granting a patent and initial rejections of the patent application seem to be the rule rather than the exception. Responses are then required to keep the patent application moving forward and to overcome the examiner's rejections.

All countries require the payment of periodic annuities or maintenance fees to keep a patent in force and over the years, this can accumulate to a significant expense. The annuity amounts increase each year and towards the end of the life of a patent, they rise to a very high level. Thus, the countries in which Acme files a patent application are carefully chosen. Additionally, annual reviews are conducted to determine whether a patent continues to provide value to the company. Those that do not are dropped. Dropping a patent involves a significant decision. Once dropped, the subject matter of a patent enters the public domain for all to use, including competitors to Acme. And once intentionally dropped, they can never be reinstated.

IV. WHO IS AN INVENTOR?

The "inventor" is the person who conceived or envisioned a novel, non obvious and useful thing. For example, Edison invented the light bulb and Marconi invented wireless. Where the entire invention is a collaborative process, each person who makes a contribution to the complete invention is an inventor.

As a first preliminary matter, only the actual inventors can be listed on a patent and all who collaborated on the idea must be listed as inventors. A patent can be held invalid if persons are listed on the patent as inventors when they in fact are not inventors. This problem can arise when a supervisor who did not contribute to the claimed invention as an inventor nevertheless requires that his or her name be included as an inventor. Further, a patent may be held to be invalid if a person who is an inventor has not been listed on the patent. This problem can arise when an inventor has left the company and the other inventors who remain at the company fail to include the former employee as an inventor in the patent.

As a second preliminary matter, only the claims of the patent determine the scope of the invention. In many cases, it is desirable to wait until the final claims have been drafted to determine who is and who is not an inventor. Further, this is an ongoing consideration. If claims must be cancelled during prosecution of the patent application at the Patent Office, inventors of those cancelled claims may need to be dropped from the patent application, unless they are inventors of one or more of the remaining claims.

Invention under the patent laws lies exclusively in conception and not in reduction to practice. The dividing line between conception and reduction to practice is not always sharply defined. Some guidance in this regard is provided by the following quotation taken from a court decision involving inventorship:

...The conception of the invention consists in the complete performance of the mental part of the inventive act. All that remains to be accomplished, in order to perfect the act or instrument, belongs to the department of construction, not invention.

Said slightly differently: It is therefore the formation, in the mind of the inventor, of a definite and permanent idea of the complete and operative invention, as it is thereafter to be applied in practice...

Joint inventorship involves two or more persons working towards a common end and producing an invention by their corroborative efforts, the conceptions of one person complementing or supplementing those of the other or others. It is not required, however, that all persons corroborating on an invention actually work together, or work on it at the same time or contribute to it equally. If an invention involves different parts or different variations, the persons involved can still be joint inventors even though they may not all have contributed to all the parts or variations. Ordinarily, however, one who merely suggests an idea or result to be accomplished, rather than the means of accomplishing the result, or one who merely provides background material or other information is not a joint inventor.

Some guidelines with respect to joint inventorship are provided in the following points from another court decision:

- A person who has merely followed instructions of another in performing experiments is not a co-inventor of the object to which those experiments are directed.
- To claim inventorship is to claim at least some role in the final conception of that which is sought to be patented.
- Perhaps one need not be able to point to a specific component as one's sole idea, but one must be able to say that without his contribution to the final conception, it would have been less efficient, less simple, less economical, less something of benefit.
- The co-inventor must have beneficially affected the final concept of the claimed invention . . .

Incidentally, from a legal standpoint, the order that inventors are listed on a patent is meaningless. An issued patent will list all the inventors on the front page of the printed patent. However, the United States Patent and Trademark Office typically prints only the first inventor's name at the top of the patent and the remaining inventors are referred to as "et al."; for example, "Smith et al." Once again, this has no legal significance. Because of this, the patent usually will then be referred to as the "Smith Patent."

In determining the order that the inventors are listed on the patent application, it is common for the inventors' supervisor to make the decision based on the weight of contribution to the patented device or method, as reflected in the claims. In case of doubt, our Acme Patent Committee will determine the order, and its decision is final.

Any questions as to who is and who is not an inventor should be referred to the Acme Legal Department. In disputed cases, the written record typically is given great weight in the determination of who is an inventor. Those persons with clearly written, dated, and witnessed laboratory notebooks, for example, are in a better position to prove inventorship than a person relying only on memory.

V. PREPARATION OF THE PATENT APPLICATION

The inventors will assist the patent attorney in the preparation of the patent application. The patent attorney will be primarily responsible for drafting the patent application, but the inventor will be required to provide considerable assistance. Your complete and prompt cooperation in assisting the patent attorney is essential to the patent process and to securing a patent on your invention.

Once filed, the patent application cannot be changed, except for limited amendments to the claims, so it is essential that the invention be completely and accurately disclosed in the patent application as it is filed. Any inaccuracies, half-correct statements, or misleading statements in the application can render an issued patent invalid. Additionally, patents are litigated in courts before juries who typically are not educated to the extent of the inventors. Thus, the patent application is written in a style that is as easy to read and understand as possible.

The assistance the inventor will be asked to provide may include:

- Reviewing the patent application to ensure that the description of the invention is accurate; and
- Assisting the patent attorney in locating and reviewing prior art (publications, patents, devices) that discloses the invention or certain elements of the invention.

Disclosure of Material Information:

The U. S. patent law requires that all individuals associated with the filing of a patent application make a full disclosure to the U.S. Patent and Trademark Office ("USPTO") of all information known to be "material" to patentability. This includes prior art, prior patents, printed publications, or, any prior public disclosure, teaching, or suggestion of the approach used in the patent application. Such information also includes offers for sale or sales by Acme of products containing the invention before prior to the filing date of the patent application. The definition of "material" to patentability has changed over the years but if there is any doubt as to whether information is material or not, it is better to disclose it.

VI. ACME PATENT COMMITTEE

The Acme Patent Committee includes representatives from the Acme Strategic Development, Marketing, Research and Development and Legal groups. Committee meetings are held periodically (recently, six times per year) and all invention disclosures are reviewed. The purposes of the Acme Patent Committee are to develop and administer patent policy and to review invention disclosures for patenting based upon such factors as commercial value, technical significance and perceived difficulty of designing around a patent. Among many other things, the Acme Patent Committee authorizes searches, discusses the status of searches, approves drafting applications and reviews the status of such applications.

As is discussed below in more detail, the Acme Patent Committee considers not only the technical merit of an invention, but also its sales potential, its manufacturability, the likely scope of patent protection that can be obtained, and the ability and cost to the company to obtain and enforce a patent on the invention. Therefore, in order to make the best possible decision about patenting a particular invention, representatives from all of the groups mentioned above are invited to attend the Acme Patent Committee meetings.

The Committee can make a number of dispositions of an invention disclosure. These are: conduct a novelty search; file a patent application; hold until further description of the invention is received; hold until further development of the invention has occurred; hold until the invention is shown to have applicability to Acme's product line; or choose to not patent an invention for the purpose of maintaining it as a trade secret, depending on the facts surrounding a particular invention.

VII. WHICH INVENTIONS WILL ACME PATENT?

There are two main competing interests in deciding whether to patent an invention. Patents are expensive to obtain and expensive to maintain in force; however, their cost can be insignificant when compared to the competitive advantage they provide for a successful product.

Therefore, the Acme Patent Committee takes great care and its members devote significant time in deciding which inventions to patent and which inventions not to patent.

Decisions on filing patent applications on inventions are made on a case-by-case basis, taking into account all relevant factors. The following are some of the criteria that support a decision to file. Generally, at least one of these criteria should be satisfied in order to justify filing.

- Likelihood of obtaining patent protection.
- The invention is currently incorporated in an Acme product.
- There is a high probability of being incorporated in a Acme product within five years as identified by the Acme technology strategy.
- Acme is committed to maintaining patent protection because of license obligations or other contractual requirements.
- Use of the invention by a competitor would present a significant competitive disadvantage to Acme (sometimes called a "blocking patent").
- There is a significant potential for out-licensing identified by Acme's technology strategy, and resources are committed to pursuing licensing.
- The invention presents significant technology unlikely to be protected as a trade secret.

VIII. WHICH INVENTIONS WILL BE FILED INTERNATIONALLY?

The Acme Patent Committee thinks and acts globally as it assesses the merits of an invention and as it applies the criteria listed in the preceding section. Once the Acme Patent Committee decides to proceed, it next applies the following considerations in selecting the countries in which patents are to be obtained:

- Sales of Acme's product currently incorporating the technology in the country;
- Sales of Acme's product incorporating the technology are probable in the country within five years;
- A product incorporating the technology is manufactured by an Acme's licensee in the country;
- A product incorporating similar technology is manufactured by a competitor in the same country (likelihood of infringement);
- The country attracts or contains competitors prone to copying inventions ("pirate" products);
- The effectiveness of protection that is afforded by the patent program in the country. For example, if the courts of a country routinely refuse to uphold patents

owned by companies of another country, it would likely not be cost effective to obtain patent protection there.

IX. PROCESS FOR PATENT FILINGS

Typically, the company files a patent application first in the United States and within one year, we file an "International Patent Application" under the Patent Cooperation Treaty ("PCT") based on that United States filing. Other filing sequences are possible, however, almost every civilized country of the world is a member of the Patent Cooperation Treaty and all will award the International Patent Application the U.S. filing date if the International Patent Application is filed within one year of the U.S. filing date.

After approximately eighteen more months (thirty months from the U.S. filing date), the international patent application must then enter the "national phase" in the individual countries or regions of the world. Any countries or regions not selected for "national phase" at this time are permanently lost for patent protection. The invention can never receive patent protection in those countries. Thus the choice of countries for international filing is extremely important. A list of all countries that are members of the Patent Cooperation Treaty is included as Exhibit C.

European Patent Applications – The EU is a "regional" filing in which one patent application is filed in the European Patent Office ("EPO"). After successful prosecution of that application, the patent may then be registered in the member EU countries. Not all European countries are members of the EU, although the large majority are. Currently, for example, Norway is not a member and patents must be filed individually in Norway to obtain patent rights there.

X. LIMITATIONS ON PUBLIC DISCLOSURE

Do not publish or publicly talk about an invention without prior approval from the Acme Legal Department. This means you should not give a medical journal an abstract anticipating future publication. It also means you should not refer to your invention in a paper delivered at a medical conference or in talks at professional meetings or when you elaborate on your talk before a professional group. You should not disclose your invention to vendors or customers, unless they have signed a so called "two-way" Confidential Disclosure Agreement (CDA).

Most countries of the world require that a patent application be filed before any disclosure, or in patent terms, "publication" of the invention. Failure to follow this rule -- for example by talking about the invention before the application is filed -- can result in no patent being available for the invention. This "no prior publication" rule is commonly referred to in Europe as "absolute novelty" of the invention. The United States permits the filing of a patent application within a grace period of one year after publication of the invention so that the inventor can attempt commercialization before having to undertake the significant expense of obtaining patent protection. However, Acme is a company that operates internationally; therefore, "absolute novelty" of its inventions is quite important. No publication of an invention should occur before a patent application has been filed or approval of the Acme Legal Department has been obtained.

Disclosure or "publication" under the patent laws can include an unrestricted (that is, not subject to a tight CDA permitting limited disclosure of material, non-public research information) oral or written discussion with someone who is not an employee of Acme, an offer for sale, or a sale of a product having the invention in it, public use, or exhibition of the invention at a trade show or in any other way, and of course, a description of the invention in a printed publication.

Because Acme is an international company with significant sales around the world, it is extremely important that no publications of inventions be made outside the company until a patent application is on file in a government patent office, which most often will be the U.S. Patent and Trademark Office. If there is any question about this requirement, contact the Acme Legal Department for guidance.

XI. ACME INVENTOR RECOGNITION PROGRAM

It is a goal of Acme to hire the best, most creative and brightest people. Such people keep Acme ahead of the competition and permit the company to provide the best products to its customers. Because we have a tradition for delivery of leading edge technology, frequently we confront issues before our competition can conceive the issues. When we solve issues before others can think of them, invention is often required. Part of creativity includes: the creativity to produce new products; the creativity to improve on existing products; the creativity to discover a market for a product not thought of before; and the creativity to solve difficult problems. It is this creativity that generates patentable inventions.

Employees who create new ideas are required to disclose those ideas to management and to assist the company in protecting those ideas through patent protection for the benefit of the company. Think of a part of your salary paying you for this creativity. A part of the process of protecting those ideas and obtaining patent protection is an Assignment of the patent rights to Acme. When the patent application has been prepared and is ready to file with the U.S. Patent and Trademark Office, the inventors will be asked to sign an Assignment of the patent rights to Acme.

In addition, Acme recognizes the employee for each patent in which he or she is named as an inventor. This recognition is in a form approved by management. Presently the recognition is the following:

- On patent application filing, each named employee receives [\$YYY]
- On patent issuance, each named employee [receives \$ZZZ] [is granted the number of Acme shares valued at \$ZZZ] along with a patent plaque. [The share grant is pre-tax and fully vests in 60 days – subject to income tax if converted to cash.]

Any questions regarding inventor recognition or assignment should be directed to the Acme Legal Department.

XII. PROTECTING PATENT RIGHTS OF ACME:

The United States has a "first-to-invent" patent system while the rest of the world has a "first-to-file" patent system. What this means is that in the U.S., one who files a patent

application first may not receive the patent. A patent applicant who files an application later may be awarded the patent if he or she can prove invention prior to the first applicant. As a result of its "first-to-invent" system, it is crucially important to be able to prove with documents who invented first in the United States. Because memories tend to fade and are sometimes unreliable, documentary proof is essential to proving who invented first. Therefore, the company has a set of guidelines to be sure that we can prove the exact date on which an invention was created in case we ever need to do so. Such documentary proof can result in an important patent being owned by Acme rather than the competition. While such documentation would seem to be burdensome at times, these procedures are not only valuable for the patent system, but are also consistent with good scientific method. Having a record of development in some detail can make the historic records much easier to produce later.

XIII. MAINTAINING LABORATORY NOTEBOOKS

Here are essential steps to be taken by Acme employees so that Acme can maximize our investment in our patents and defend ourselves should competitors challenge our inventions:

- Make and preserve good records, following this procedure.
- Record your ideas in a laboratory notebook.

A) Laboratory Notebook Contents

Here are some specific guidelines and practical ideas to help you maintain laboratory notebooks that will help us protect our valuable IP assets. In general, the laboratory notebook must be bound and must not allow the addition or removal of pages without it being obvious that pages have been added or removed. The covers of the laboratory notebook must be large and sturdy enough to protect the inner pages. All pages must be numbered and must be strong enough in construction to withstand much usage without tearing out of the book. Each page must have a location at the bottom for two signatures and dates and a location at the top for a description of the project. In addition:

- As soon as practicable after thinking of an idea, enter your conception of the invention in your laboratory notebook in its practical application and in terms as broad as you think will work.
- Describe your work in such a way that someone outside Acme who has a comparable background could understand it.
- Write as legibly as possible.
- Whenever possible, use permanent ink.
- Date each record.
- Sign each record.
- Have your records countersigned and dated promptly. Ideally, the counter-signer is one who observed the work being recorded. The next best is one who works in the same department. In any case, the counter-signer should be one who

understands the work, but is not a potential co-inventor. A witnessed, dated signature testifies to the fact that the record existed at that point in time and may serve, at a later time, to refresh the recollection of the witness who signed.

- Clearly identify materials used and their source. Give full identification of any Acme-prepared material, including lot number. Specify the source of other materials where practical.
- Pages should be used consecutively. Any unused page or major portion of a page should have a diagonal line through it. Sign and date these pages also.
- Record all observed data of importance, even if negative. Make careful statements when wording conclusions.
- Alterations of any kind should be avoided, but, if necessary, they should be explained, signed, dated, and witnessed. Use one-line cross-outs, not obliterations.
- If a Acme code name or number is assigned to an invention, this name or number should be recorded in a conspicuous place on the laboratory notebook page.
- If notes in the margin are used, they should be dated, signed, and witnessed.
- Set aside time to record your work and to counter-sign co-worker's records; this is expected as part of your job.
- It is helpful if the book is indexed. The index may be started on the top of the last page and continued on the next page toward the back of the book using as many pages as are necessary.

B) Datasheets and Attachments

- It is frequently desirable to incorporate a datasheet, such as a photograph or computer printout, into the laboratory notebook record.
- If the data sheet is not bulky, it should be affixed to a separate page or blank portion of a page. White glue should be used (scotch tape and rubber cement deteriorate with time and should be avoided).
- Reference the attachment in the text; initial and date just below the attachment.
- If the data sheet is bulky (for example, a lengthy computer printout), you may keep it in a separate binder as long as your laboratory notebook entry references the data sheet by subject matter, date, run or other codes sufficient to clearly identify the data sheet, and the laboratory notebook also indicates where the original data sheet can be found. Be sure to retain the data sheet as back-up for the laboratory notebook entry.

C) Control of Laboratory Notebooks

The assignment of laboratory notebooks to individual users is handled as follows: [insert which department is responsible for keeping a library of laboratory notebooks]. Each laboratory notebook will have a unique identification number. The respective departments will keep records of which laboratory notebook was assigned to whom. All laboratory notebooks belong to Acme, and will be kept by the assigned individual, until his/her employment is terminated. The user must not allow anyone else to write in his or her laboratory notebook, except as a witness to the user's work. Each employee is responsible for maintaining the laboratory notebook until it is full, until he or she is assigned to another department or until the employee leaves the company, at which time all laboratory notebooks in their possession will be turned over to the company.

- Laboratory notebooks that are no longer in active use must be sent to the _____ Department for storage.
- LABORATORY NOTEBOOKS AND ALL OTHER RECORDED DATA ARE THE PROPERTY OF THE COMPANY. SHOULD YOU LEAVE THE COMPANY, DO NOT TAKE LABORATORY NOTEBOOKS OR OTHER RECORDED DATA, OR ANY COPIES OF THESE, WITH YOU.

XIV. INVENTION DISCLOSURES

Complete the invention disclosure form as soon as you believe your invention will work for its intended purpose. A copy of the invention disclosure form is attached as Exhibit D and can be found by going to the employee intranet site.

From the Intranet, the invention disclosure may be downloaded as an MS Word document and completed locally. Extra paper copies are available from the Acme Legal Department if needed. The time for completing the form may be immediately after recording your conception, if no testing or checking is necessary to prove the invention will work; or it may be at a later stage when sufficient work has been done to confirm that your invention does what you say it will do. If you have doubts as to when to file the invention disclosure form or what information to supply, contact the Acme Legal Department.

XV. AVOIDING PATENT INFRINGEMENT

It is the strict policy of Acme that the valid patent rights of others will not be violated.

Therefore, as soon as practicable after a product has been identified for development or improvement, a "right-to-use" or "freedom to operate" search should be conducted to determine the extent of the patent rights of others. Contacting the Acme Legal Department with a description of the product and the present schedule of development will commence this process.

Once the right-to-use study is begun, a search will be conducted and relevant patents in the field obtained. Copies of these patents will be forwarded to the responsible project manager and will be reviewed in parallel by a patent attorney. After the patents have been reviewed, further searching may be performed or the involved persons may meet to discuss in detail the extent of the patent rights of others shown in those patents. In appropriate cases, the Acme Legal Department may request an opinion letter for the patent attorney before further development occurs.

XVI. PUBLICLY AVAILABLE SOURCES OF INFORMATION

The following sites on the World Wide Web are available to the public for patent information. In most cases, patent applications, as well as issued patents, are available. Searches may be conducted and copies of patents may be made.

- a. Australia – see www.ipaustralia.gov.au/
- b. Canada – see www.cipo.gc.ca/
- c. Europe – see <http://ep.espacenet.com/>
- d. United Kingdom – see www.patent.gov.uk/
- e. United States – see www.uspto.gov/

XVII. FURTHER QUESTIONS

Any questions should be directed to the Acme Legal Department.

EXHIBIT C

PATENT COOPERATION TREATY
MEMBER LISTING
(as of August 2003)

- A Albania, Algeria, Andorra, Angola, Antigua and Barbuda, Argentina, Armenia, Australia, Austria, Azerbaijan
- B Bahamas, Bahrain, Bangladesh, Barbados, Belarus, Belgium, Belize, Benin, Bhutan, Bolivia, Bosnia and Herzegovina, Botswana, Brazil, Brunei Darussalam, Bulgaria, Burkina Faso, Burundi
- C Cambodia, Cameroon, Canada, Cape Verde, Central African Republic, Chad, Chile, China, Colombia, Congo, Costa Rica, Côte d'Ivoire, Croatia, Cuba, Cyprus, Czech Republic
- D Democratic People's Republic of Korea, Democratic Republic of the Congo, Denmark, Djibouti, Dominica, Dominican Republic
- E Ecuador, Egypt, El Salvador, Equatorial Guinea, Eritrea, Estonia, Ethiopia
- F Fiji, Finland, France
- G Gabon, Gambia, Georgia, Germany, Ghana, Greece, Grenada, Guatemala, Guinea, Guinea-Bissau, Guyana
- H Haiti, Holy See, Honduras, Hungary
- I Iceland, India, Indonesia, Iran (Islamic Republic of), Iraq, Ireland, Israel, Italy
- J Jamaica, Japan, Jordan
- K Kazakhstan, Kenya, Kuwait, Kyrgyzstan
- L Lao People's Democratic Republic, Latvia, Lebanon, Lesotho, Liberia, Libyan Arab Jamahiriya, Liechtenstein, Lithuania, Luxembourg
- M Madagascar, Malawi, Malaysia, Mali, Malta, Mauritania, Mauritius, Mexico, Monaco, Mongolia, Morocco, Mozambique, Myanmar
- N Namibia, Nepal, Netherlands, New Zealand, Nicaragua, Niger, Nigeria, Norway
- O Oman
- P Pakistan, Panama, Papua New Guinea, Paraguay, Peru, Philippines, Poland, Portugal
- Q Qatar
- R Republic of Korea, Republic of Moldova, Romania, Russian Federation, Rwanda
- S Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Samoa, San Marino, Sao Tome and Principe, Saudi Arabia, Senegal, Serbia and Montenegro, Seychelles, Sierra Leone, Singapore, Slovakia, Slovenia, Somalia, South Africa, Spain, Sri Lanka, Sudan, Suriname, Swaziland, Sweden, Switzerland

EXHIBIT C

PATENT COOPERATION TREATY
MEMBER LISTING
(as of August 2003)

T	Tajikistan, Thailand, The former Yugoslav Republic of Macedonia, Togo, Tonga, Trinidad and Tobago, Tunisia, Turkey, Turkmenistan
U	Uganda, Ukraine, United Arab Emirates, United Kingdom, United Republic of Tanzania, United States of America, Uruguay, Uzbekistan
V	Venezuela, Viet Nam
Y	Yemen
Z	Zambia, Zimbabwe

EXHIBIT D

INVENTION NAME:

ACME TECHNOLOGY, CO.

INVENTION DISCLOSURE

Patents are very important to Acme Technology, Co ("Acme"). They give Acme the right to prevent others from *making, using, selling, offering to sell or importing* the new technologies created at Acme for a limited time. Patents may be obtained to protect many different inventions ranging from mechanical devices, to electronic circuitry, to software, to new drugs, to living organisms. Under the patent laws, processes, machines, manufactures, compositions of matter, or any new and useful improvements are patentable "inventions".

Obtaining a patent is a complicated procedure that can be considerably eased by filing a patent application that includes a straightforward story about the invention or discovery based on the following elements:

- A. The problem that the invention solves;
- B. A brief history of what others in the field have done to solve the same problem, i.e., the prior art;
- C. A detailed description of the invention and at least one "embodiment" or application of the invention; and
- D. The advantages of the invention over the prior art.

The inventor is usually the person who is most able to furnish this story, and it should be reported in accordance with the outline of information set forth on the following Invention Disclosure form.

Please complete the Invention Disclosure form and attach all necessary details as appropriate. You may attach copies of other materials, such as laboratory notebook pages, if you believe they would provide a clearer description or picture of the invention. The last page of the Invention Disclosure requests that you provide an abstract of your disclosure. The abstract is used for reference purposes to facilitate processing. Samples are given. Once the form is completed, please submit it to:

Note: Please do not disclose or publish any aspects of this invention or discovery without prior approval from the Acme Legal Department. Also, witnesses signing the Invention Disclosure must be persons other than the Inventor(s).

ACME TECHNOLOGY, CO.
INVENTION DISCLOSURE FORM

INVENTOR(S) NAMES – Provide the names and associated information of the person(s) believed to be Inventor(s).

FULL Name of Primary Contact: _____

Complete Residence Address: _____

Citizenship: _____

Telephone: (W) _____ (Cell) _____ Fax: _____
(H) _____ E-mail: _____

Second Inventor - Full Name: _____

Complete Residence Address: _____

Citizenship: _____

Telephone: (W) _____ (Cell) _____ Fax: _____
(H) _____ E-mail: _____

Third Inventor - Full Name: _____

Complete Residence Address: _____

Citizenship: _____

Telephone: (W) _____ (Cell) _____ Fax: _____
(H) _____ E-mail: _____

Fourth Inventor - Full Name: _____

Complete Residence Address: _____

Citizenship: _____

Telephone: (W) _____ (Cell) _____ Fax: _____
(H) _____ E-mail: _____

DESCRIPTIVE TITLE OF INVENTION

PROBLEM SOLVED BY THE INVENTION - What is the invention intended to accomplish?

What problem does it solve?

PRIOR ART - Describe known prior art, devices, systems, and methods used to solve the same problem. Discuss the drawbacks to those prior art approaches.

DESCRIPTION OF THE INVENTION

The following requested information should be in the inventor's own words, supplemented by sketches, engineering drawings, pages from laboratory notebooks, photographs, etc., which should be attached to this disclosure. If reports are available, they should be attached, and referred to where appropriate. Extra numbered sheets should be used if more space is needed, and each extra sheet should be signed and dated.

- A. General area, product line or technology where the invention fits:

- B. Describe in detail the construction and operation of an embodiment or application of your invention, point out the advantages it has, and emphasize any important features. Write your description using reference numerals placed on sketches, drawings, or photographs attached. Point out and explain relationships with associated equipment:

- C. Describe specific structural and operation features of the invention that are believed to be new:

- D. Describe any alternative (in structure or method) that would function in substantially the same way to give substantially the same results as the device or method described above:

ADVANTAGES OF THE INVENTION OVER THE PRIOR ART - Explain briefly the advantages your invention has over the prior approaches discussed above in Section IV.:

CONCEPTION OF THE INVENTION

- A. What date did you first think of (conceive) this invention?

B. What records do you have to substantiate this conception date, including record books, letters, notes, drawings, reports, etc? (Identify such records and their location. State the date of the first drawing, if any):

- _____
- (i) Date of first drawing(s):

- (ii) Who has custody of the first drawing(s):

- (iii) Date of first notes or written description:

- (iv) Who has custody of the first notes or written description:

- (v) Date of first oral disclosure to others:

- (vi) To whom first oral disclosure was made:

- (vii) Place first oral disclosure made:

REDUCTION TO PRACTICE OF THE INVENTION

- A. Have you done any actual experimental work toward carrying out the invention? Identify any laboratory notebooks that document efforts at reducing the invention to practice. If so, on what date did you begin work: _____ and what date was the first working prototype completed: _____
- B. Who made the first working prototype:

- C. Who has custody of the first working prototype:

- D. Test of Invention:
 - (i) Date of test(s) of invention: _____
 - (ii) Place tested: _____
 - (iii) Who tested the invention: _____
 - (iv) Names of witnesses to test(s): _____

IX. DOCUMENTATION OF THE INVENTION AND PUBLICATION, MARKETING EFFORTS, USE, OR SALE

- A. Identify photographs or test reports made. Who has custody of the photographs or test reports:

- B. Date of first (actual or planned) field trials:

- C. Date of first (actual or planned) presentation at a trade show or seminar:

- D. Date of first (actual or planned) disclosure outside of the company:

- E. Date of first (actual or planned) publication and name of publication:

- F. Date of first offer for sale. Name of first purchaser or user.

- G. Any samples of the invention been distributed, if so, to whom and when:

X. WHAT IS THE PRESENT STATUS OF THE INVENTION

XI. LITERATURE AND PATENT REFERENCES - Identify known related publications, patents, or patent applications. Extra numbered sheets should be used if more space is needed, and each extra sheet should be signed and dated.

XII. ABSTRACT - Please provide a brief abstract of your invention below. It should include the new features of the invention that distinguish it from the prior art. A sample abstract is provided below.

Sample - [insert sample of one of the company's patent abstracts]

ABSTRACT:

INVENTOR(S) SIGNATURE(S):

By: _____ Date: _____
 Typed Name:

By: _____ Date: _____
 Typed Name:

By: _____ Date: _____
 Typed Name:

By: _____ Date: _____
 Typed Name:

WITNESSED AND UNDERSTOOD:

By: _____ Date: _____
 Typed Name:
 (Not an Inventor)

By: _____ Date: _____
 Typed Name:
 (Not an Inventor)

SAMPLE ONLINE PRIVACY POLICY

[E-COMMERCE COMPANY, MULTIPLE SITES, CALIFORNIA PRESENCE, COPPA-EXEMPT]

privacy policy

Overview

Provide Commerce, Inc. ("Provide Commerce," "we" or "us") is committed to protecting our customers' privacy. We feel it is important that you fully understand the terms and conditions under which we use the information we gather from you through the use of each of our websites located at, or linked to, the URLs www.proflowers.com, www.uptownprime.com, www.cherrymoonfarms.com, www.secretspoon.com, www.providecommerce.com and www.prvd.com, and through the use of any of our co-branded sites we maintain with one or more of our business partners (which website contains a link to this privacy policy or whose URL address contains any of the root URLs "www.proflowers.com/", "www.cherrymoonfarms.com/", "www.uptownprime.com/", "www.secretspoon.com/", "www.providecommerce.com/" or "www.prvd.com/") (collectively, our "Sites"). Please read this privacy policy ("Policy") carefully to understand how we will use and protect your personal information. We will never share your personal information with anyone except as described in this Policy. Changes to this Policy will be announced on each of our Sites at least ten (10) days in advance, so please check back periodically.

Questions regarding this Policy should be directed to info@providecommerce.com or we may also be contacted directly at the following address:

Attn: Office of the General Counsel
 Provide Commerce, Inc.
 5005 Wateridge Vista Drive
 San Diego, CA 92121

This Policy will explain the following regarding use of each of our Sites:

1. What Personally Identifiable Information do we collect from you?
2. Where do we collect information from you and how do we use it?
3. Who is collecting your information?
4. With whom do we share your information?
5. How may you update, correct or delete your Personally Identifiable Information?
6. What are your choices regarding collection, use and distribution of your information?
7. What security precautions are in place to protect against the loss, misuse or alteration of your information under our control?
8. Cookies/clear GIFs.
9. Children, parental consent and privacy.
10. You should carefully review privacy policies of any third-party sites accessible from any of our Sites and any co-branded websites not covered by this Policy.
11. Contacting us about privacy questions or concerns.
12. Policy changes.

1. What information does Provide Commerce collect from or about you?

In order to better provide you with numerous products and services, each of our Sites collects two types of information about its visitors: Personally Identifiable Information and Non Personally Identifiable Information. Our primary goal in collecting information from you is to provide you with a smooth, efficient and customized experience while using our Sites.

Personally Identifiable Information: "Personally Identifiable Information" refers to information that lets us know the specifics of who you are and can be used to identify, contact or locate you. Personally Identifiable Information is requested when you register with us, order a product or service, fill out surveys, participate in contests or sweepstakes, correspond with us, or otherwise volunteer information, for instance, through the use of one of our greeting, hint or reminder services. Personally Identifiable Information might include your name, mailing address, telephone number, mobile phone number, email address, and other identification and contact information. If you are using a greeting, hint or reminder service on one of our Sites, we may ask you to provide the name, mailing address, email address, telephone number, mobile phone number, age, date of birth, anniversary date or other personal annuity date of you, a friend, a loved one, family members or other third parties, and certain holiday information that may reveal one's religious background, so that we may send them or you a hint or reminder about an event that could be made more special with the gift of our products. We may also collect certain financial information, like your credit card number (or a check or money order if using such payment method while ordering via mail); whenever we do so, we will attempt to provide a link to this Policy so that you can confirm how this information will be used. With this information, we can fill your service and product orders and better provide you with personalized services. You also may have the option of importing information into certain Sites from third-party software. This information may include these categories, as well as other categories of information that you have entered into these third-party programs.

Non Personally Identifiable Information: "Non Personally Identifiable Information" refers to information that does not identify a specific individual by itself or in combination with other information. We may gather certain information about you such as age, date of birth, gender, anniversary date or other personal annuity date of you, a friend, a loved one, family members or other third parties, certain holiday information that may reveal one's religious background, as well as consumer purchasing information based upon where you shop on any one of our Sites. This information may be compiled and analyzed on both a personal and an aggregated basis. This information may include the website's Uniform Resource Locator ("URL") that you just came from, which URL you next go to, what browser you are using, and your Internet Protocol ("IP") address. A URL is the global address of documents and other resources on the Internet. An IP address is an identifier for a computer or device on a Transmission Control Protocol/Internet Protocol ("TCP/IP") network, such as the Internet. Networks use the TCP/IP protocol to route information based on the IP address of the destination. In other words, an IP address is a number that is automatically assigned to your computer whenever you are surfing the Internet, allowing Internet servers to locate and identify your computer. Computers require IP addresses in order for users to communicate on the Internet, browse and shop.

2. Where do we collect information from you and how do we use it?

Our primary goal in collecting personal information is to provide our visitors with a superior customized online experience. We use customer contact information to fill orders, contact prior purchasers to inform them of their order status, to remind customers of events through our reminder service(s), to send our customers' friends or loved ones greetings or hints to send our products through a greeting or hint service, and to send service and promotional emails.

We may perform statistical analyses of aggregate customer behavior. This allows us to measure relative customer interest in the various areas of each of our Sites for product development purposes. Any information we collect is used for our own internal purposes to improve the content and navigation of our

Sites, to enhance users' experiences when visiting our Sites, to customize the content and/or layout of our pages, and to provide the services required by an individual customer. We also use information to notify consumers about updates to our Sites, to complete user initiated transactions, to trace false orders and to contact consumers directly, or through our third-party service partners, for marketing purposes.

We gather information in the following ways:

Shopping: We collect IP addresses for the purposes of system administration, to gather broad demographic information, and to monitor the level of activity on our Sites. We collect information from visitors to each of our Sites regarding the referring URL, your IP address, which browser you used to come to any one of our Sites, the country, state and telephone area code where your server is located, and the pages of any one of our Sites that you viewed during your visit.

Ordering: When you order from us, we collect Personally Identifiable Information from you. If you order one of our products or services, we will collect and maintain your name, email address, mailing address, telephone or mobile number, product selections, credit card number (or check or money order information if using such payment methods while ordering via mail), order number, referring URL, IP address and a password, as well as the recipient's name, address, telephone or mobile number and email address. We collect this, and other information, as disclosed in this Policy, in order to fill your order, to communicate with you about your order, or the recipient, as appropriate, and to send you promotional materials. Before confirming your order, you will have the opportunity to review the product order form and make changes and additions to the information it contains and these changes will be automatically kept for future use. If you cancel an order or do not complete an order we may collect and use any email address or other information that you have entered as we would collect and use it if you had completed an order.

When an order is placed for delivery to you by a third party we need to collect Personally Identifiable Information regarding such third party to fulfill the order. Such information includes their name, address, telephone or mobile number and email address.

Track/Modify Order: If you use our Track & Modify Your Order service we will gather your email address and account password, if you have one, in order to locate your order so that we may give our most recent tracking information, or so that you may modify the order. If you choose to modify your order, we may collect information that we would normally collect when you order products, as explained in the above paragraph.

Notices to Recipients: If you are a recipient of an order placed by a third party we may send one or more emails regarding such order, including regarding customer service issues. In addition, we may send you additional emails in compliance with applicable laws in order to promote our Sites and services and to seek your consent to opt in to receive our various newsletters, promotional emails and other services. If we send you emails notifying you of an order, or that promote our Sites and services, they will contain an opt out link or email address. We may also telephone you regarding the shipment of your order. You can also opt out of receiving newsletters, promotions, non-transactional related emails or phone calls from us hereunder by calling us at 800-210-2279 or by sending an email to us at unsubscribe@providecommerce.com.

Corporate Account: When you set up a corporate account with us or when you contact us to inquire about corporate programs (either via email, telephone, letter or our online web forms), we collect your name, company name, email and telephone or mobile number. We may add you to a list for future newsletters and promotions regarding corporate sales. Upon signing up for a corporate account we will contact you by either email or telephone to determine how we can best serve your corporate needs. We will also give you the opportunity to receive periodic updates regarding our corporate services. If you make purchases through your corporate account we shall gather similar information that we gather when you order as an individual, plus certain information regarding your corporation. You can opt out of

receiving newsletters, promotions, non-transactional related emails or phone calls from us hereunder either while you are completing our online web form, by calling us at 800-210-2279 or by sending an email to us at unsubscribe@providecommerce.com.

Surveys and Polling: In order to improve our services to you, we ask some of our customers or product recipients to voluntarily complete surveys online or via telephone, which may be collected by an independent third party. Individual survey answers are confidential, although Non Personally Identifiable Information may be collected and disclosed to third parties. If you do not wish to participate in a survey, simply decline to participate when asked.

Contests and Sweepstakes: We may from time to time conduct contests or sweepstakes. Customers who choose to participate may be asked to provide Personally Identifiable Information. That information may then be used by us for such purposes as notifying winners and fulfilling promotional obligations as well as providing electronic newsletters and promotional emails for our products and/or services (which you can opt out of receiving as described more fully below).

Newsletters & Promotional Emails: We may offer free electronic newsletters and promotional emails for products and/or services offered on any one or more of our Sites as a service to our prior customers from any of our Sites. We may send you newsletters and emails periodically listing current specials and deals from us or through our third-party service partners. However, you will have the choice to opt out of receiving newsletters and promotional emails for products and/or services offered on any one or more of our Sites. Once we have processed your request, we will not send you promotional emails with respect to products and/or services offered by us through the particular Site(s) of which you had opted out unless you opt back in to receiving such communications directly or by making an additional purchase or attempted purchase on one of our Sites. There may be opportunities to subscribe to an email list that will send you information about the events on our Sites, but we will only add you to the list with your consent. To stop receiving our newsletters that pertain to any one or more of our Sites, send an email to us at unsubscribe@providecommerce.com.

Cookies/Clear GIFs: In conjunction with our third-party service partners, we make limited use of cookies and clear GIFs to gather information when you visit any one of our Sites, make a purchase and when you click through to any one of our Sites from a targeted email, newsletter or partner site. We may also use cookies and clear GIFs to gather and compile such information about you when you return to our Sites so that we may better customize our services to you. To find out what cookies and clear GIFs are and how they can be used, please refer to Section 8 of this Policy below.

Contact Information and Third-Party Data: If you contact us by telephone, email or letter, we may keep a record of your contact information, correspondence or comments. If you report a problem with any one of our Sites, we may collect such information in a file specific to you. If you provide us feedback through any one of our Sites, by email or by calling one of our customer service representatives, we may ask for your name and email address in order to send you a reply. If other users or third parties send us correspondence about your activities or purchases on any one of our Sites, or if you are the recipient of products sent by another customer, we may keep the information in a file specific to you. If you are using a greeting, hint or reminder service on one of our Sites, we may ask you to provide the name, mailing address, email address, telephone number, mobile phone number, age, date of birth, anniversary date or other personal annuity date of you, a friend, a loved one, family members or other third parties, and certain holiday information that may reveal one's religious background, so that we may send them or you a hint or reminder about an event that could be made more special with the gift of our products. We store this information for the purpose of sending one or more emails in connection with such an event. You, the loved one, friend, family member, or other third party, may contact us at info@providecommerce.com to request the removal of this information from our database.

Greeting, Hint and Reminder Services: If you choose to use a greeting, hint or reminder service on one of our Sites, we may ask for and store your name, email address, mailing address, telephone number, mobile phone number, age, date of birth, gender, certain holiday information that may reveal one's religious background and other identification and contact information. We may ask you to provide the name, mailing address, email address, telephone number, mobile phone number, age, date of birth, anniversary date or other personal annuity date of you, a friend, a loved one, family members or other third parties, and certain holiday information that may reveal one's religious background, so that we may send them or you a hint or reminder about an event that could be made more special with the gift of our products.

Mobile Phone Reminders: You may have the option of receiving reminders of holidays and other dates on your mobile phone through a text messaging or email notification service (collectively, the "Mobile Phone Reminders"). By signing up for Mobile Phone Reminders you are indicating your agreement with the rules and conditions listed below, as well as the applicable terms and conditions for such service. If you sign up for Mobile Phone Reminders, you will need to provide us with your mobile phone number. Moreover, by signing up for this service you consent to receive messages and emails on your mobile phone from Provide Commerce (or one of our third-party agents acting on our behalf) that may contain commercial content. If you do not wish to receive such messages or services, please do not register for Mobile Phone Reminders. Moreover, you agree that you will only provide Provide Commerce with your mobile phone number, and not that of a third party. By signing up you will be receiving messages on your mobile phone from Provide Commerce (or one of our third-party agents acting on our behalf). You may be charged by your wireless service provider in connection with the receipt of these messages. In addition, any Mobile Phone Reminders that you receive may offer you an opportunity to request further information or to make a purchase via a phone line or through another medium via your mobile phone, whereby special rates to be charged by your mobile operator may apply. You may terminate Mobile Phone Reminders at anytime upon request by sending an email to us at friends@reminderspot.com.

Affiliate and Partnership Programs: You may purchase products from us through a link on one of our affiliates' ("Affiliates") websites. We pay each Affiliate a commission, or a portion of the sales made to those who link to our Site(s) from the Affiliate's site. Some of our Affiliates run a "rewards" or "charity" program (the "Programs"). Under such Programs, participants receive credits based on the commissions an Affiliate receives from sites such as ours. Participants in such programs can donate their credits to a chosen charitable organization, or keep them for their own use and benefit. If you come to our Sites through an Affiliate's site, make a purchase from us, and you are a participant in such Programs, we may share your name, e-mail address and the value of your purchases, including that data necessary for Affiliates to credit participants with purchases made under their Program, with a third-party service partner, primarily Commission Junction, which collects data for our standard Affiliate program. In addition to Commission Junction, we may also share such information with other third-party Affiliates if you have registered with their affiliate, affinity or rewards programs, and that Affiliate has made sales for you, processed your order and/or if such third-party Affiliate directed you to one of our Sites.

With respect to our co-branded Sites maintained by us in conjunction with our business partners, we may share information collected by us to our business partners under our separate agreements with them. These business partners may use your personal information to help us communicate with you about offers from us as well as offers from such partners. However, if you opt out of receiving newsletters and promotional emails from us, you will automatically opt out of receiving newsletters and promotional emails from such business partners through their use of personal information which we collected from you on our co-branded Sites and which we provided to such business partners. We may ask you to share your information with such business partners via an opt in or opt out request on such Sites. Please note that with respect to personal information our third-party business partners may collect from you independent of us and outside the scope of co-branded Sites maintained by us on our servers, we will have no control

over the use of such information by such third-party business partners and the use and gathering of such data will be subject to the third party's privacy policies.

Registering for an Affiliate Program: Please read the terms of our Affiliate Program Agreement. A record of any and all information submitted to us as part of an Affiliate Program application shall be stored by us and only disclosed by us in an effort to evaluate such application with prior consent from you.

We also track customers' traffic patterns throughout their online sessions, including which pages a customer views while using our Sites. We use your IP address to diagnose problems with our servers and software and to administer our Sites.

We may share aggregated statistics about pages viewed on our Sites and sales and other shopping information with third parties.

3. Who is collecting your information?

Except as otherwise expressly discussed in this Policy, only we collect your information. This Policy only addresses the use and disclosure of information we collect from you. We encourage you to ask questions and to be very cautious before you disclose your Personally Identifiable Information to others. Our third-party advertising service partner may collect information about you through the use of cookies or clear GIFs when you click on its advertisements, open promotional emails or newsletters or visit our Sites via a link in a promotional email or newsletter. This information is gathered solely for our use, however, our third-party advertising service partner may use this information in a non personally identifiable aggregated form for its own purposes. You should contact our third-party advertising service partner directly if you have any questions about its use of the information that it collects. For more information about how our current primary third-party advertising service partner collects information please click here: http://www.doubleclick.net/us/corporate/privacy/privacy/email/default.asp?asp_object_1=8.

From time to time, we may utilize the services of third-party survey providers that may collect Personally Identifiable Information from you for certain services, including voluntary surveys that are conducted on our behalf and certain of our reminder services. This may include information regarding you, as well as third parties about whom you provide information. If you chose to participate in these surveys, or use these services, this Personally Identifiable Information may be stored on the servers of the third-party survey providers used by us, but this Personally Identifiable Information will remain the sole property of us and will be handled in accordance with this Policy.

We also utilize third-party providers for our same-day florist delivery service, wine sales and certain date collection and reminder services. We make sure to disclose such relationships to you on the website pages where any such information is being collected from you. Unless otherwise disclosed to you, any such third-party providers collect information from you solely on our behalf.

In addition, we currently employ one or more third-party service partners that track the traffic on our Sites. However, the only information that may be gathered by such third parties is Non Personally Identifiable Information with the exception of email addresses. For more information about how our third party service partner tracks traffic on our sites, as well as information on how to opt-out of certain aspects of such tracking, please click here: <http://www.websidestory.com/privacy/privacy-policy.html>.

4. With whom do we share your information?

Except as otherwise stated in this Policy, we do not sell, trade or rent your Personally Identifiable Information collected on our Sites to others. The information collected by our Sites is used to process orders, to keep you informed about your order status, to notify you of products or special offers that may be of interest to you, and for statistical purposes for improving our Sites. We will disclose your Personally

Identifiable Information to third parties for tracking purposes, to charge your credit card (or process your check or money order, as appropriate), fill your order, improve the functionality of our Sites, customize our marketing efforts with you and perform statistical and data analyses, deliver your order and deliver promotional emails to you from us. These third parties may not use your Personally Identifiable Information other than to provide the services requested by us. For example, we must release your credit card number to confirm payment and release your mailing address information to the delivery service to deliver products that you ordered. We also share website usage information we gather from visitors to our Sites who have received a targeted promotional campaign with our third-party advertising service partner for the purpose of targeting future campaigns and upgrading visitor information used in reporting statistics. For this purpose, we and our third-party service partners note some of the pages you visit on any one of our Sites through the use of clear GIFs. For more information about our primary third-party advertising service partner, please click here:

http://www.doubleclick.net/us/corporate/privacy/privacy/email/default.asp?asp_object_1=8.

From time to time we may disclose certain information (names, postal addresses and non-sensitive transactional information such as your purchase history, amounts paid and products ordered) to direct marketing companies for trade or rental purposes. You may "opt out," or instruct us not to distribute such information to third parties in the future by sending an email with such instructions to info@providecommerce.com; however, we may not be able to provide you our full range of services if we cannot distribute certain Personally Identifiable Information.

In certain circumstances under California law, customers of Provide Commerce are entitled to certain information regarding any personally identifiable information (as defined by certain California laws) we may share with direct marketing companies. Personally identifiable information generally is defined under California law as information that identifies specifics about an individual and can be used to identify, contact, or locate an individual including that individual's name, mailing address, telephone number, mobile phone number, email address and other identification and contact information. If you are an eligible customer of Provide Commerce and would like to receive a list detailing the types of personally identifiable information we share with direct marketing companies and the names and addresses of all direct marketing companies that we provide personally identifiable information to, please email us at info@providecommerce.com. We will respond to any request for information at such email address within thirty (30) days.

We may provide aggregated statistics about our customers, sales, traffic patterns, and related Site information to third parties that do not include Personally Identifiable Information. Moreover, we may release account information when we believe that such release is reasonably necessary to enforce or apply our Terms and Conditions of Use or to protect the rights, property and safety of our users, others and ourselves.

Recipient Requests: From time to time we are contacted by flower and other gift recipients who ask us who the sender was. If we receive a request from a recipient asking who sent flowers or another gift we will provide the name and any other information as contained on the gift message accompanying the flowers or gift. If there is no gift message filled out or if there is no name on the gift message we may ask the sender via email. If we receive approval to disclose the sender's name from the sender via email or in writing, we will then inform the recipient. If the sender does not reply via email or in writing or if the sender denies permission, then we will not reveal the sender's identity to the recipient.

Enforcement of Law: From time to time, we may be required by law enforcement or judicial authorities to provide Personally Identifiable Information to the appropriate governmental authorities. We will disclose Personally Identifiable Information upon receipt of a court order or subpoena or to cooperate with a law enforcement investigation. We fully cooperate with law enforcement agencies in identifying those who use our services for illegal activities. We reserve the right to report to law enforcement agencies any activities that we in good faith believe to be unlawful.

Merger and Acquisitions: In the event of a merger, consolidation, or sale or transfer of all or substantially all of the assets or business of Provide Commerce, Inc. (a "Successor"), one of the assets which would generally be transferred is the information we collect from our customers. However, the use of this information by any Successor would still be governed by the terms of this Policy, as amended from time to time, including any amendment after such transaction, and you will continue to have the right to opt out of sharing your information with third parties.

5. How can you update or correct your Personally Identifiable Information?

During the online ordering process you can review, change or delete the information that you have submitted. We are updating our Sites so that you may change any of your personal information in your account(s) online at any time. You may ask us in writing via mail or email at info@providecommerce.com to have the information on your account deleted, updated or corrected; however, because we keep track of past purchases, you cannot delete information associated with past purchases. Note that we may retain changed or deleted information for archival or other purposes.

6. What are your choices regarding collection, use and distribution of your information?

We may from time to time send you email or other communications regarding current promotions, specials and new additions to our Sites. If you have supplied us with your telephone number(s) you may receive telephone calls from us with information or requests for information regarding an order you have placed. You may "opt out," or unsubscribe from our newsletters and non-transactional related emails by following the unsubscribe instructions in any email you receive from us or by sending an email to unsubscribe@providecommerce.com. If you make a purchase or an attempted purchase on one of our Sites, you will be opted back in to our newsletters and promotional communications until you opt out or unsubscribe once again.

If you are using a greeting, hint or reminder service on one of our Sites, then you may have the option of sharing your Personally Identifiable Information and Non Personally Identifying Information, as well as information that you have entered regarding third parties, with others. If you share this information with third parties, these parties are not bound to follow this Policy and may disclose or use this information in ways we will not.

7. What security precautions are in place to protect against the loss, misuse or alteration of your information?

We employ reasonable security measures to protect the security of the information you submit to us. The importance of security for all Personally Identifiable Information associated with our customers is of utmost concern to us. Our secure servers protect this information using password protection and advanced encryption, and we may use firewall technology for additional protection.

In order to most efficiently serve you, credit card transactions and order fulfillment are handled by established third-party banking institutions, process agents and distribution institutions. They receive the information they need to verify and authorize your credit card transactions and to ship your order. When collecting credit card information for online purchases, we offer secured server transactions that encrypt your information in transit to thwart someone from intercepting it and misusing it. When you access your account information, the information is kept on a secure server. Furthermore, all of the customer data we collect is protected against unauthorized access by physical security means.

We also encourage our partners and service providers to adopt and follow stringent consumer privacy policies.

8. Cookies/clear GIFs.

Cookies: Like many other commercial sites, our Sites utilize standard technologies called "cookies" and clear GIFs to collect information about how each of our Sites is used. A cookie is a small data text file, which a website stores on your computer's hard drive (if your web browser permits) that can later be retrieved to identify you to us. Cookies were designed to help a website recognize a user's browser as a previous visitor and thus save and remember any preferences that may have been set while the user was browsing the site. A cookie cannot be read by a website other than the one that set the cookie. Cookies can securely store a customer's password, personalize home pages, identify which parts of a site have been visited or keep track of selections, such as those selected in a "shopping cart." For instance, cookies allow us to prepopulate (or fill in) an email field with your email address if you revisit one of our Sites and place an order. A cookie cannot retrieve any other data from your hard drive, pass on a computer virus, or capture your email address.

We send a cookie to your hard drive when you make an order to record the product name, category of product that you ordered, the amount paid, the order number and any referral codes. No Personally Identifiable Information is recorded. When you click through to any one of our Sites from a promotional email, our third-party advertising service partner may send a cookie to your hard drive recording your IP address and other related information.

Clear GIFs: We currently work with third-party service partners that employ clear GIFs (also known as pixel tags, single pixel GIFs, web beacons or action tags) for our benefit to help us measure advertising effectiveness. Clear GIFs help us better manage content on our Sites by informing us of what content is effective. Clear GIFs are tiny graphics with a unique identifier, similar in function to cookies, and are used to track the online movements of our users. The main difference between the two is that clear GIFs are invisible on the page and are much smaller, about the size of the period at the end of this sentence. Clear GIFs are not tied to your Personally Identifiable Information.

Our third-party service partners use clear GIFs: (i) in HTML based emails to let us know which emails have been opened by recipients; (ii) to record when products have been ordered from our Sites; and (iii) to track the visitor traffic on our Sites. These clear GIFs allow us to measure the usage of each of our Sites by our visitors and the effectiveness of certain communications and marketing campaigns. We may also use clear GIFs in a similar manner in our own emails and on our Sites.

Clear GIFs can "work with" existing cookies on a computer if they are both from the same website or advertising company. That means, for example, that if a person visited "www.companyX.com", which uses an advertising company's clear GIF, the website would match the clear GIFs identifier and the advertising company's cookie ID number, to show the past online behavior for that computer. This collected information can be shared with the advertising company. We do provide such information to our third-party advertising service partners, but that information can only be used by our partner for our benefit. For more information about our primary third-party advertising service partner, please click here: http://www.doubleclick.net/us/corporate/privacy/privacy/email/default.asp?asp_object_1=8.

9. Children, parental consent and privacy.

The Children's Online Privacy Protection Act took effect on April 21, 2000, and imposes certain requirements on websites directed toward children under 13 that collect information on those children, or on websites that know they are collecting Personally Identifiable Information from children under the age of 13. We want to let you know that it currently is our policy not to collect Personally Identifiable Information from any person under 13 because children are not permitted to use the Sites or services on the Sites, and we request that children under the age of 13 not submit any personal information to us via the Sites. As one measure to ensure that we do not gather Personally Identifiable Information from children, we require that all individuals provide a valid credit card number before completing a purchase

order. If we learn that we have inadvertently gathered Personally Identifiable Information from children under 13, we shall attempt to notify such child's parent or guardian and erase such information from our records, unless the child's parent or guardian consents to our maintaining such information. Our greeting, hint or reminder services are designed not to gather birthdates (with years) or other personal information directly from children under 13. However, there may be instances where you will be allowed to enter birthdates (with years) for children under 13 while using one of our greeting, hint or reminder services whereby no Personally Identifiable Information other than name may be linked to such child. This process is designed so that we will not knowingly market to such children under 13 while being able to provide you with increased functionality for our greeting, hint or reminder services.

10. You should carefully review privacy policies of any third-party sites accessible from any of our Sites and any co-branded websites not covered by this Policy.

Other sites accessible through any of our Sites have their own privacy policies and data collection, use and disclosure practices. Please consult each site's privacy policy. We are not responsible for the policies or practices of third parties. Please be aware that our Sites may contain links to other sites on the Internet that are owned and operated by third parties. The information practices of those websites linked to our Sites are not covered by this Policy. These other sites may send their own cookies or clear GIFs to users, collect data or solicit Personally Identifiable Information. Additionally, other companies which place advertising on our Sites may collect information about you when you view or click on their advertising through the use of cookies or clear GIFs. We cannot control this collection of information. You should contact these advertisers directly if you have any questions about their use of the information that they collect.

We also may have co-branded websites that are maintained by us in connection with one or more of our third-party business partners but which do not contain this Policy or a link to this Policy. When you submit information to one of these co-branded sites you may be submitting it to both Provide Commerce and our third-party business partners or just to our third-party business partner. Note that these co-branded sites may contain, or link to, privacy policies that contain terms and conditions different than those contained in this Policy. Again, this Policy only pertains to the information Provide Commerce collects and we are not responsible for the privacy policies or practices of our business partners. We encourage you to read the privacy policies of those co-branded sites so that you will always know what information we gather and what information is gathered by our third-party business partner, how each of us might use that information, to whom each of us will disclose it and what choices you have.

11. Contacting us about privacy questions or concerns.

If you have any questions about this Policy, the practices of any of our Sites, or your dealings with any of our Sites, please contact us by sending a letter to: Office of the General Counsel, Provide Commerce, Inc., 5005 Wateridge Vista Drive, Second Floor, San Diego, CA 92121, or by sending an email to info@providecommerce.com.

12. Policy changes.

This Policy was last changed on December 30, 2005. If we make changes to any terms or conditions of the Policy, the changes will be posted on this portion of the Sites so that you will always know what information we gather, how we might use that information, to whom we will disclose it and what choices you have. Any change, modification, addition or removal of portions of this Policy will be announced on our Sites at least ten (10) days before it is implemented. Please be sure to check this page before proceeding to use any of our Sites.

[privacy](#) | [terms](#) | © 1998-2006 Provide Commerce, Inc. All rights reserved.

SAMPLE ONLINE TERMS & CONDITIONS

[E-COMMERCE COMPANY, MULTIPLE SITES, CALIFORNIA (& MULTI-STATE) PRESENCE, DMCA-COMPLIANT]

terms and conditions of use

The following rules ("Terms and Conditions") govern the use of each of the websites located at, or linked to, the URLs www.proflowers.com, www.uptownprime.com, www.cherrymoonfarms.com, www.secretspoon.com, www.providecommerce.com and www.prvd.com, and the use of any of our co-branded websites that we maintain with one or more of our business partners (which website contains a link to these Terms and Conditions) and the services that may be offered on each of the sites; our greeting, hint, reminder or Track & Modify Your Order services; our Affiliate Program(s) and corporate accounts; the ability to order products and receive newsletters and promotional emails; and any related links (collectively, our "Sites"). Please read the following Terms and Conditions carefully.




By using any one of our Sites, you understand and expressly agree to be legally bound by these Terms and Conditions and our [Privacy Policy](#) and to follow these Terms and Conditions and all applicable laws and regulations governing our Sites. The Terms and Conditions shall supersede any subsequent terms or conditions included with any purchase order, whether or not such terms or conditions are signed by Provide Commerce, Inc. ("Provide Commerce," "we" or "us"). We reserve the right to change these Terms and Conditions at any time, effective immediately upon posting on our Sites. If you violate these Terms and Conditions, we may terminate your use of the Sites, bar you from future use of the Sites, and/or take appropriate legal action against you.

Copyrights and Trademarks of Provide Commerce

Each of our Sites is owned and operated by us. Unless otherwise specified, all materials appearing on our Sites, including the text, site design, graphics, logos, icons and images, as well as the selection, assembly and arrangement thereof, are the sole property of Provide Commerce, Inc., © 1998-2006, ALL RIGHTS RESERVED. All audio and video clips are the sole property of Provide Commerce or our respective content providers. The content and software on our Sites is the property of Provide Commerce and/or its suppliers and is protected by U.S. and international copyright laws. You may view, download, print and retain a copy of pages of any of our Sites only for your own personal use. Except as expressly provided above, you may not use, download, upload, copy, print, display, perform, reproduce, republish, license, post, transmit or distribute any information from any of our Sites in whole or in part without our prior written permission. If you wish to obtain permission to reprint or reproduce any materials appearing on any one of our Sites you may contact us at info@providecommerce.com. All rights not expressly granted herein are reserved.

We post legal notices and various credits on pages of each of our Sites. If you duplicate, publish or otherwise distribute material on any of our Sites, you may not remove these notices or credits or any additional information accompanying such notices and credits.

The following is a list of trademarks, trade names and service marks owned by Provide Commerce:

PROVIDE COMMERCESM, PROFLOWERS®, CHERRY MOON FARMSSM, SECRET SPOONSM, UPTOWN PRIME®, UPTOWN CATCHSM, THE ART OF FRESHER FLOWERSSM, DIRECT FROM THE FIELDSSM, FLOWERFARM.COM®, FRESHNESS FACTOR®, ENJOY FLOWERS!®, FLOWER FARM DIRECT®, PQUADSM, REWARDS IN BLOOMSM, REMINDER SPOTSM, SM, SM and [®].

The absence of a trademark, trade name or service mark from the above list does not constitute a waiver of our intellectual property rights concerning that trademark, trade name or service mark. All custom graphics, icons, logos and words listed above are trade names, trademarks or service marks of Provide Commerce. All other trade

names, trademarks or service marks are property of their respective owners. The use of any of our trade names, trademarks or service marks without our express written consent is strictly prohibited. In order to maintain the value of these marks, it is important that they are used correctly. If you have any questions, you may contact us at info@providecommerce.com.

Permitted Use

You agree that you are only authorized to visit, view and to retain a copy of pages of the Sites for your own personal use, and that you shall not duplicate, download, publish, modify or otherwise distribute the material on the Sites for any purpose other than for personal use, unless otherwise specifically authorized by us to do so. You also agree not to deep-link to the site for any purpose, unless specifically authorized by us to do so. The content and software on the Sites are the property of Provide Commerce and is protected by U.S. and international copyright laws.

Copyright Policy

We may terminate the privileges of any user who uses the Sites unlawfully to transmit copyrighted material without a license, express consent, valid defense or fair use exemption to do so. If you submit information to the Sites, you warrant that the information does not infringe the copyrights or other rights of third parties.

Representations by You

By visiting any of the Sites, you represent, warrant and covenant that (a) you are at least 18 years old; (b) that you are a resident of the United States; and (c) that all materials of any kind submitted by you through the Sites or for inclusion on the Sites will not plagiarize, violate or infringe upon the rights of any third-party including trade secret, copyright, trademark, trade dress, privacy, patent, or other personal or proprietary rights.

Accounts

During the registration process you will be asked to select a unique password for access to certain portions of the Sites. You are responsible for maintaining the confidentiality of the password and account, and are fully responsible for all activities that occur under the password. By logging into the Sites, you represent and warrant that: (i) you are the customer who registered for the services; (ii) that you are using the services only for permitted purposes; (iii) you are not a competitor of Provide Commerce, or agent thereof; (iv) you will immediately notify us of any unauthorized use of the password or account or any other breach of security; and (v) you will ensure that you exit from your account at the end of each session. Please notify us at info@providecommerce.com of any potential unauthorized use(s) of your account, or breach of security.

You also represent and warrant that: (i) you will not select or utilize a user name of another person with intent to impersonate that person; (ii) you will not select or utilize a user name in which another person has rights, if you do not have that person's authorization to use such name; and (iii) you will not select or utilize a user name that Provide Commerce in its sole discretion deems offensive.

Typographical Errors

In the event a product (including, but not limited to, flowers, plants, floral arrangements, fruits and meat products) is listed at an incorrect price or with incorrect information due to typographical error or error in pricing or product information received from our suppliers, we shall have the right to refuse or cancel any orders placed for products listed at the incorrect price. We shall have the right to refuse or cancel any such orders whether or not the order has been confirmed and your credit card charged. If your credit card has already been charged for the purchase and your order is canceled, we shall immediately issue a credit to your credit card account in the amount of the charge.

Order Acceptance Policy

Your receipt of an electronic or other form of order confirmation does not signify our acceptance of your order, nor does it constitute confirmation of our offer to sell. We reserve the right at any time after receipt of your order to accept or decline your order for any reason. We reserve the right at any time after receipt of your order, without prior notice to you, to supply less than the quantity you ordered of any item. We may require additional verifications or information before accepting any order.

Sales Taxes

We shall automatically charge and withhold the applicable sales tax for orders to be delivered to addresses within California, Colorado, Florida, Georgia, Indiana, Kansas, Kentucky, Massachusetts, Minnesota, Mississippi, New Jersey, North Carolina, Ohio, Pennsylvania, Rhode Island, Tennessee, Texas, Virginia and Washington. Each customer shall be solely responsible for all sales taxes, or other taxes, on orders shipped to any other state. Notwithstanding the foregoing, sales tax will not be applicable with respect to orders on uncooked meat products from our www.uptownprime.com Site (except for residents of Tennessee).

Specials, Promotions and Sweepstakes/Contests

Please read the official rules that accompany each special offer, coupon, discount, contest and sweepstakes that we may offer or conduct.

Links and Search Results

Each of our Sites may link to other sites operated by third parties. We have no control over other sites or their content and cannot guarantee, represent or warrant that the content of these sites is accurate, legal and/or inoffensive. We do not endorse the content of other sites, and cannot warrant that these sites do not contain viruses or other features that may adversely affect your computer. By using any one of our Sites to search for or link to another third party site, you agree and understand that you may not make any claim against us for any damages or losses resulting from your use of our Site to obtain search results and/or to link to a third party site. However, if you have a problem with a link from any one of our Sites, please notify us at info@providecommerce.com. We will investigate the link and take appropriate action.

Violation of the Terms and Conditions

By using any one of our Sites, you understand and agree that we, at our sole discretion and without prior notice, may terminate your access to one or more of our Sites and to any services offered on our Sites, and may remove any content on any of our Sites you have provided ("User Content") if we believe that the User Content violates or is inconsistent with these Terms and Conditions or their intent, that your conduct is disruptive, or you have violated the law or the rights of Provide Commerce or another user.

License Granted by You

By providing User Content to us, which includes submitting or uploading content or materials for use on the Sites, you represent and warrant that you or the owner of all rights to such content or materials has expressly granted us an irrevocable worldwide right in all languages and in perpetuity to use and exploit all or any part of the content and materials provided by you. We may publish and distribute any such submitted content or materials at our sole discretion by any method now existing or later developed. You agree that you shall waive all claims and have no recourse against us for any alleged or actual infringement or misappropriation of any proprietary rights in any communication, content or material submitted to us. Any communication or materials you send to us will be treated as non-confidential and non-proprietary and may be disseminated or used by us for any purpose, including, but not limited to, developing, creating, manufacturing or marketing products or services.

Compliance With Laws

You agree to comply with all applicable laws, statutes, ordinances and regulations regarding your use of our Sites and your purchase of products or services through our Sites. We may, in our sole discretion, report actual or perceived violations of law to law enforcement or appropriate authorities. If we become aware, through a complaint or otherwise, of any potential or suspected violation of these Terms and Conditions or our privacy policy ("Privacy Policy"), we may (but are not obligated to) conduct an investigation to determine the nature and extent of the suspected violation and the appropriate enforcement action, during which investigation we may suspend services to any customer being investigated and/or remove any material from our servers. You agree to cooperate fully with any such investigation. You acknowledge that violations of the Terms and Conditions or the Privacy Policy could be subject to criminal or civil penalties.

Export

The United States export control laws regulate the export and re-export of technology originating in the United States. This includes the electronic transmission of information and software to foreign countries and to certain foreign nationals. You agree to abide by these laws and their regulations.

Privacy

We respect and make efforts to protect the privacy of all users of our Sites. Our current Privacy Policy available at <http://www.providecommerce.com/privacy.aspx> is incorporated herein by reference and made a part of the Terms and Conditions.

DMCA Policy

If you are notifying Provide Commerce of alleged copyright infringement, please be sure to provide the following information in the form required by 17 USC Section 512:

1. A description of the copyrighted work that you allege is being infringed, or, if multiple copyrighted covered by a single notification, a representative list of such works;
2. A description of the allegedly infringing material and information sufficient to permit us to locate the material;
3. Information reasonably sufficient to permit us to contact you, such as an address, telephone number, and/or an electronic mail address;
4. A statement by you that you have a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, or its agent, or the law; and
5. A statement by you that the information in the notification is accurate and that you have the authority to enforce the copyrights that are claimed to be infringed.

Designated Agent for Notification of Claimed Copyright Infringement

NAME: Blake T. Bilstad, Esq.
 ADDRESS: Office of the General Counsel
 Provide Commerce, Inc.
 5005 Wateridge Vista Drive
 San Diego, CA 92121
 EMAIL: legal@providecommerce.com
 PHONE: 858-638-4900
 FAX: 858-638-4708

Feedback

We welcome all comments, feedback, information, or materials ("Feedback"), which you submit to us by email or otherwise through or in conjunction with any one of our Sites. Please note that Feedback shall be considered non-confidential and become the property of Provide Commerce. By submitting Feedback to us, you agree to a no charge assignment to us of all right, title and interest in copyrights and other intellectual property rights on a worldwide basis to the Feedback. We shall be free to use Feedback on an unrestricted basis.

Restrictions

You must be 18 years or older and have a valid credit card, with full authority to use it, to submit an order through any of our Sites. You agree not to use any of our Sites or any content contained in it for any illegal or inappropriate activities.

Shipping and Delivery

Provide Commerce, in conjunction with our service providers, will attempt to deliver a product on the requested day. Our service providers do not telephone prior to delivering packages, and we cannot guarantee the time of delivery.

Provide Commerce is not responsible for:

- Flowers, plants, fruits, meat products and preserved items delivered to incorrect addresses supplied by the sender.
- Unsuccessful deliveries arising from the recipient not being present at time of delivery at the address supplied by the sender.
- Decreased product quality due to an incorrect delivery address supplied by the sender, or a re-route requested by the sender.
- Product quality problems caused by improper handling by the recipient.

Free shipping offers are valid only on weekday deliveries to addresses within the Continental United States.

Orders

Provide Commerce does not allow orders to be edited or cancelled within forty-eight (48) hours of the requested delivery date, or within the seven (7) days prior to Thanksgiving, Christmas, Valentine's Day or Mother's Day, because of our extremely high volume of orders during these times.

Special offers, coupons, or discounts cannot be used in conjunction with other offers. Limit one promotion per order.

Guarantee and Disclaimers

PROVIDE COMMERCE GUARANTEES THAT (A) ITS FLOWERS, PLANTS, AND PRESERVED ITEMS ORDERED ON THE WWW.PROFLOWERS.COM SITE WILL BE FRESH FOR AT LEAST SEVEN (7) DAYS AFTER DELIVERY; AND (B) YOU WILL BE COMPLETELY SATISFIED WITH ANY FRUIT PRODUCTS ORDERED ON THE WWW.CHERRYMOONFARMS.COM, ANY CHOCOLATE OR CONFECTION PRODUCTS ORDERED ON THE WWW.SECRETSPOON.COM SITE AND ANY MEAT OR SEAFOOD PRODUCTS ORDERED ON THE WWW.UPTOWNPRIME.COM SITE. WITH RESPECT TO EITHER OF OUR GUARANTEES, OUR SOLE MAXIMUM LIABILITY WILL NOT BE MORE THAN TO REFUND THE PURCHASE PRICE OR TO REPLACE AND DELIVER EQUIVALENT PRODUCT ITEMS, AS APPROPRIATE, AS SOON AS REASONABLY POSSIBLE. THE APPLICABLE

GUARANTEE MUST BE BROUGHT WITHIN THIRTY (30) DAYS AFTER DELIVERY OR WE SHALL NOT BE LIABLE AND YOU WILL HAVE WAIVED ANY AND ALL RELATED CLAIMS REGARDING SUCH PRODUCT ITEMS.

WHILE WE ENDEAVOR TO PROVIDE THE MOST ACCURATE, UP-TO-DATE INFORMATION AVAILABLE, THE DIRECTORIES AND INFORMATION ON OUR SITES MAY BE OUT OF DATE OR INCLUDE OMISSIONS, INACCURACIES OR OTHER ERRORS. OUR SITES AND THE MATERIALS THEREIN ARE PROVIDED "AS IS" AND "AS AVAILABLE." WE DO NOT PROMISE THAT OUR SITES OR ANY SERVICES OFFERED ON OUR SITES WILL BE ERROR-FREE OR UNINTERRUPTED, OR THAT THE USE OF OUR SITES OR ANY CONTENT, SEARCH OR LINK ON THEM WILL PROVIDE ANY SPECIFIC RESULTS.

EXCEPT AS EXPRESSLY STATED HEREIN, WE EXPRESSLY DISCLAIM ALL REPRESENTATIONS, GUARANTEES, WARRANTIES, EXPRESS OR IMPLIED, OF ANY KIND WITH RESPECT TO PRODUCTS SOLD ON OUR SITES, OUR SITES AND OUR SITES' USE, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you. You may have other rights which vary from jurisdiction to jurisdiction.

Limitation of Liability

YOU AGREE THAT, EXCEPT AS EXPLICITLY SET FORTH HEREIN, PROVIDE COMMERCE, ITS DIRECTORS, OFFICERS, EMPLOYEES OR OTHER REPRESENTATIVES SHALL NOT BE LIABLE FOR DAMAGES RELATED TO PRODUCTS SOLD OR THE OPERATION, CONTENT OR USE OF OUR SITES. YOU AGREE THAT THIS LIMITATION OF LIABILITY IS COMPREHENSIVE AND APPLIES TO ALL DAMAGES OF ANY KIND, INCLUDING WITHOUT LIMITATION DIRECT, INDIRECT, COMPENSATORY, SPECIAL, INCIDENTAL, PUNITIVE AND CONSEQUENTIAL DAMAGES, DAMAGES FOR LOSS OF PROFITS, REVENUES, DATA AND USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, RELATED TO OUR PRODUCTS OR YOUR ACCESS TO, AND USE OF, OUR SITES OR ANY OTHER HYPER-LINKED THIRD PARTY WEB SITE, EVEN IF WE HAVE BEEN ADVISED OF, OR ARE AWARE OF, THE POSSIBILITY OF SUCH DAMAGES.

Because some states/jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

Mobile Phone Reminders

You may have the option of receiving reminders of holidays and other dates on your mobile phone through a text messaging or email notification service (collectively, the "Mobile Phone Reminders"). By signing up for Mobile Phone Reminders you are indicating your agreement with the rules and conditions listed below, as well as the applicable terms and conditions for such service. If you sign up for Mobile Phone Reminders, you will need to provide us with your mobile phone number. Moreover, by signing up for this service you consent to receive messages and emails on your mobile phone from Provide Commerce (or one of our third-party agents acting on our behalf) that may contain commercial content. If you do not wish to receive such messages or services, please do not register for Mobile Phone Reminders. Moreover, you agree that you will only provide Provide Commerce with your mobile phone number, and not that of a third party. By signing up you will be receiving messages on your mobile phone from Provide Commerce (or one of our third-party agents acting on our behalf). You may be charged by your wireless service provider in connection with the receipt of these messages. In addition, any Mobile Phone Reminders that you receive may offer you an opportunity to request further information or to make a purchase via a phone line or through another medium via your mobile phone, whereby special rates to be charged by your mobile operator may apply. You may terminate Mobile Phone Reminders at anytime upon request by sending an email to us at friends@reminderspot.com.

Advertising

The Sites may contain advertisements and/or sponsorships. The advertisers and/or sponsors that provide these advertisements and sponsorships are solely responsible for insuring that the materials submitted for inclusion on the Site are accurate and comply with all applicable laws. We are not responsible for the acts or omissions of any advertiser or sponsor.

Applicable Law

You agree that any legal action brought against us shall be governed by the laws of the State of California, without regard to conflict of law principles. You agree that the sole jurisdiction and venue for any litigation arising from your use of or orders made on any one of our Sites shall be an appropriate federal or state court located in San Diego County, California. We make no representations that the content in our Sites is appropriate for access outside the United States. Those who choose to access any one of our Sites from outside the United States do so on their own initiative and are responsible for compliance with local laws. If any provision within the Terms and Conditions is held to be invalid or unenforceable, such provision shall be struck and all remaining provisions shall be enforced.

Indemnity

By using any one of our Sites, you agree to indemnify and hold Provide Commerce, its subsidiaries, affiliates, officers, agents and other partners and employees, harmless from any loss, liability, claim or demand, including reasonable attorneys' fees, made by any third party due to or arising out of your use of such Site, including providing a link to another site or uploading any content to such Site.

Severability

If any provision of the Terms and Conditions is held to be invalid, void or unenforceable, the remaining provisions shall nevertheless continue in full force and effect.

Headings

Section titles in the Terms and Conditions are for convenience and do not define, limit, or extend any provision of the Terms and Conditions.

How to Contact Us

If you have any comments or questions, please do not hesitate to contact us at info@providecommerce.com or at 1-800-776-3569, or write us at:

Office of the CEO
Provide Commerce, Inc.
5005 Wateridge Vista Drive
San Diego, CA 92121

[privacy](#) | [terms](#) | © 1998-2006 Provide Commerce, Inc. All rights reserved.

Technology Systems Contracting Checklist

- Scope Completion
- Functional Specifications Completion
- Technical Specifications Completion
- Inspection Timetable
- Testing Schedule
- Go-Live Date and Punchlist Procedure
- Coordination with Related Agreements
- Milestones
- Compensation Structure
- Service Levels
- Interim and Final Acceptance
- Testing Exhibit
- Staffing
- Reporting
- Change Management Procedure
- Operational Dispute Resolution

Technology Systems Contracting Checklist (cont.)

- IP Due Diligence
- Warranty
- Maintenance Arrangement
- Who Can Use
- IP Rights
- Contractor Confidentiality Obligations
- Customer Confidentiality Obligations
- General Indemnity
- Infringement Indemnity
- Insurance
- Service Level Credits
- Limits of Liability
- Source Code Escrow
- Termination for Convenience
- Termination Fees
- Transition

Technology Systems Contracting Considerations

1. Scope of Work and Implementation Schedule

a. Proposal vs. Scope

- Just the facts, but plenty of them
- Who owns the SOW?
- Planning for technology changes
- Breakable pieces
- Avoid joint responsibilities

b. Functional Specifications Complete

- Possible to include as attachment to SOW?
- If not, set early deadline
- Minimize exit cost if no agreement reached

c. Technical Specifications Complete

- Possible to include as attachment to SOW?
- If not set deadline well before scheduled Go Live Date
- Minimize exit cost if no agreement reached

d. Inspection Dates

- Onsite at Contractor's facility early in development
- Third Party inspection rights

e. Testing Schedule

- Keep it linear
- Synchronize with Acceptance and Milestones

f. Go-Live Date

- Handling "punch list"
- Customer flexibility
- Compensation holdback

2. Milestones

- Financial teeth vs. Moral outrage
- Timing
- Tie to Acceptance
- Tie to Compensation

3. Compensation Structure

- T & M-Unlimited or against a maximum?
- Tied to Milestones
- Avoiding illusory limits
- License fee treatment

4. Warranty and Maintenance

a. General Warranty

- Tie to SOW and documentation

b. Service Levels

- Liquidated Damages
- Keep it simple
- Keep goals in sight-aggregate picture vs. individual hot buttons

#187795

#187795

c. Maintenance Obligations

- Long term options
- Updates vs. Upgrades
- Level of Effort

5. Testing and Acceptance

- Create procedures clients can follow
- What is the record
- Avoid endless approval loop
- Stay in that loop
- Interim acceptances where appropriate

6. Project Management

a. Staffing

- Prior Approval vs. subsequent veto
- Impact on compensation

b. Reporting

- Interplay with Milestones and Acceptance

c. Change Management

- Change orders vs. Amendments
- Compensations structure
- Stay in the loop

d. Operational Dispute Resolution

- Involve appropriate departments

#187795

7. Intellectual Property Rights

a. Contractual Allocation

- Inventions vs. Pre-Existing
- Focus on real needs
- Defensive vs. offensive
- Need to modify
- Scope of use vs. Assignment

b. Due Diligence

- Patent searches
- Interplay with indemnity and creditworthiness

8. Confidentiality Obligations

a. IP

- Interplay with IP ownership
- Third Party Access

b. Data

- Timeframe

c. General

- Remember statutory protection
- Making/identification requirements

#187795

9. Indemnification

a. General

- Intentional/negligence vs. breach
- Avoid overlaps
- Interplay with limits of liability

b. Infringement/IP

- The dreaded trio of remedies

c. Insurance

- Professional vs. General Liability

10. Remedies

a. Service Level Credit

- Interplay with broader remedies
- Interplay with limits of liability

b. General

- Litigation concerns
- Credit Enhancements
- Source Code Escrow

c. Limits of Liability

- Qualitative vs. quantitative
- Tool of necessity vs. tool of convenience
- When=how much

11. Termination

- For convenience
- Termination fees
- As a remedy
- Transition

12. Coordination with Related Agreements

- General Contractor vs. System Integrator vs. Running your own show
- Shared risk
- Synchronized Acceptance, Testing and Milestones
- Suspension rights

#187795

#187795



10 Nuggets

- 1. Identify Inventions Early and Often
- 2. Coming to Terms with Open Source
- 3. Co-Development – Who Owns What?
- 4. NDAs – The Crippling Effect
- 5. E-Commerce Primer
- 6. Obey Your Privacy Policies
- 7. Secure all Content – Watch Out for Music & Video
- 8. Don't Run an Illegal Lottery
- 9. Smart Coordination of IT Implementation
- 10. Pay to Motivate Performance

ACC's 2006 Annual Meeting: The Road to Effective
Leadership

October 23-25, Manchester Grand Hyatt



#1 – Identify Inventions Early & Often

- Who Invents?
 - R&D
 - Others in the company – Marketing / CEO
 - 3rd Parties who are Work for Hire
- Make sure ALL sign Invention Assignment Agreements
 - Assign ownership of Inventions to the Company
 - Make Part of Employment Agreements and Consulting/Service Agreements

ACC's 2006 Annual Meeting: The Road to Effective
Leadership

October 23-25, Manchester Grand Hyatt



#1 - Identify Inventions Early & Often

- Confidentiality - Why Important?
 - US: File within 1 year from 1st Public Disclosure
 - Europe: File before 1st Public Disclosure
- Confidential Disclosure Agreements
 - Employees
 - Share ideas outside of the Company (e.g. thought leaders, customers)
 - Make them specific to the topic - create evidentiary trail



#1 - Identify Inventions Early & Often

Takeaway:

- Make Inventions & Patenting a Process
 - Patent Manual
 - Invention Assignments
 - Invention Disclosure
 - Patent Committee
 - Patent Recognition Program



#2 - Coming to Terms with Open Source

- What is Open Source Software?
- What are the risks associated with using Open Source?
- Why is your business strategy so important?
- What steps do companies take to manage the risks associated with Open Source?



#3 – Co-Development – Who Owns What?

- “Work for Hire” or “Co-Development”?
- Desired Outcome may be vague & discovered only during the R&D effort
- Contract is a Work Plan
 - Sets the Rules of How the Parties will work together
 - Sets the Rules for Determining Who will Own What
 - What did each Party come to the table with at the beginning?
 - What is each Party expected to contribute along the way?



#3 – Co-Development – Who Owns What?

● Important Contract Provisions

- Team / Team Lead
- Milestones (Deliverables & Timing)
- Responsibilities of each Party
- IP Ownership
 - I own “My stuff” / You own “Your stuff”
 - Assignment clauses
 - We both Jointly Own the New Stuff
 - Co-operate in Patent Prosecution
 - One of us owns the New Stuff and Licenses it to the Other
 - Royalty rate or free? Exclusive / Non-exclusive / Non-compete?
- What is the on-going relationship post-development?



#3 – Co-Development – Who Owns What?

Takeaways:

- Be involved early in strategy development
- Question R&D and Marketing In Detail
- Get your IP house in order before opening discussions
- Follow progress of development closely
 - Are there detailed records of who invented what?
 - Who owns invention under the rules of the contract??



#4 - NDAs: The Crippling Effect

- General
 - Remember statutory protection
“Trade secret” means information, including a formula, pattern, compilation, program, device, method, technique, or process, that:
 - (1) Derives independent economic value from its disclosure or use; and obtain economic value from its disclosure or use; and
 - (2) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.
California Civil Code Section 3426.1
 - Marking/oral or written identification requirements



#4 - NDAs: The Crippling Effect

- IP
 - Interplay with IP~ Make sure you can use what you own or license
Ensure Deliverables can be fully used
 - Marking/oral or written identification requirements
- Access
 - Third Parties
 - Affiliates



#5 - E-Commerce Primer

- Document your online transactions and policies
 - Terms and Conditions of Use
 - ⊗ Conduct of consumers
 - ⊗ IP notices; DMCA compliance
 - Privacy Policy
 - ⊗ Data collected; Uses of such data
 - ⊗ Security procedures
 - ⊗ Children

#5 - E-Commerce Primer

- Always play the role of the consumer.
- What are they seeing and agreeing to as they navigate your site and access new features?
- Are these policies and practices reasonable, legal?



#6 – Obey Your Privacy Policies

- Beware False Promises re: Privacy
- Ultimately Four Issues:
 - What information do you collect?
 - What do you do with the information?
 - When can't you disclose it.
 - When must you disclose it.



#6 – Obey Your Privacy Policies

- Federal Privacy Statutes:
 - Children's Online Privacy Protection Act (COPPA)
 - Gramm-Leach-Bliley (financial)
 - Electronic Communications Privacy Act (ECPA)
 - Identity Theft and Deterrence Act
 - Health Insurance Portability and Accountability Act (HIPAA – medical)
 - Others (FCRA, RACTA)
- Other Jurisdictions Also Regulate



#6 – Obey Your Privacy Policies

● Privacy Takeaways

- Assess what info you collect, draft policies that are consistent with the laws, and obey them!
- Reserve the right to modify your policies
- Determine if you are sending or receiving data to jurisdictions (*e.g.*, European Union) that have higher privacy and security standards



#7 – Secure All Content

● Acquiring or Licensing Certain Types of Multimedia Content Can Be Tricky

- *e.g.*, Music, Video, Motion Pictures
- Varies by country as well!
- For music rights in the U.S., must consider the interlocking rights of sound recording owners and publishers with two types of performance rights and two types of copyrights – can be 4 different parties involved with each work!
 - Record Labels, Harry Fox Agency, individual artists/publishers, ASCAP/BMI/SESAC



#7 – Secure All Content

- Online content aggregators wise to use blanket form agreements with “teeth” and flexibility to copyright issues
- Negotiating rights with entertainment conglomerates will involve significant legal resources
- Consult An Expert When Licensing Multimedia



#8 – Don't Run an Illegal Lottery

- Three questions to ask:
 - Is there a PRIZE?
 - Is there CHANCE involved?
 - Is there CONSIDERATION?
- If answer is “Yes” to all three questions, then you are conducting an illegal lottery.



#8 – Don't Run an Illegal Lottery

- Exceptions usually come under consideration issue (*e.g.*, AMOE)

- State and local laws vary (*e.g.*, NY, FL, AZ, Quebec), so consult expert counsel when running prize promotions



#9 - Smart Coordination of IT Implementation

- SOW
 - The devil is in no details
 - Severable is preferable
 - Teamwork vs. Accountability
 - Functional vs. Technical
 - Looking over the vendor's shoulder
 - Go-Live Date



#9 - Smart Coordination of IT Implementation

- Testing and Acceptance
 - Synchronized Acceptance, Testing and Milestones
 - Avoid endless approval loop
 - Interim acceptances where appropriate
 - Create Procedures clients can follow

#9 - Smart Coordination of IT Implementation

- Vendor's Role
 - General Contractor vs. System Integrator vs. Running your own show
 - Shared risk
 - Related Agreements
 - Suspension rights



#10 - Pay to Motivate Performance

- Milestones with teeth
- The horrors of T&M
- The NTE Illusion
- License fees: the foot in the door
 - General Contractor vs. System Integrator vs. Running your own show
 - Shared risk
 - Related Agreements
 - Suspension rights

ACC's 2006 Annual Meeting: The Road to Effective Leadership

October 23-25, Manchester Grand Hyatt

#10 - Pay to Motivate Performance

- Service Levels
 - Liquidated Damages
 - Keep it simple
 - Keep goals in sight-aggregate picture vs. individual hot buttons
- Warranty and Maintenance Issues

ACC's 2006 Annual Meeting: The Road to Effective Leadership

October 23-25, Manchester Grand Hyatt