EMPLOYEE ACKNOWLEDGMENTS

- ✓ Code of Conduct
- ✓ Use of Computer Systems Policy
- ✓ Nondisclosure Agreement
- ✓ Business Driver Policy

CODE OF CONDUCT

1. Introduction

a. Inform Diagnostics, Inc., along with its subsidiaries and affiliates (the "Company") is committed to providing quality pathology services to our customers while observing the highest standards of legal and business ethics. This Code of Conduct (the "Code") forms the foundation of the Company's overall compliance efforts which seek to ensure continuing compliance with all applicable laws, rules and regulations that govern our business operations. The Code applies to all employees, independent contractors, vendors, and suppliers and serves as a guide for our day-to-day activities. It does not, however, address every situation that may arise. Specific guidance is available from the Corporate Compliance Officer ("CCO"), Human Resources, Legal Department and senior management. Employees have the responsibility of initiating action to seek counsel for activities that may be violating the Code or Company policies and procedures.

b. Compliance is critical to the Company because we are a visible and important industry leader and because our daily business impacts many lives. The Company has a successful reputation as a recognized national industry leader in quality, service and technology in the laboratory industry. Our history of integrity in our business practices instills confidence in our clients. It also differentiates us from, and represents a significant challenge to, our competitors. A violation of the Code or Company policies and procedures is considered serious, and may result in disciplinary action up to and including termination of the person engaging in the violation.

2. Quality of Care and Services

a. The Company will provide services that conform to superior clinical and safety standards and employees are responsible for maintaining integrity and quality in their job performance.

3. Business Ethics and Legal Compliance

a. The Company will conduct its business ethically and honestly, following both the letter and spirit of applicable law and regulations. The Company complies with federal regulations regarding government contracts and programs in which it participates. Employees will not make any verbal or written false statements to a government payor or other payor. Employees will not enter into any joint ventures, partnerships or other risk- sharing arrangements with any entity that is a potential or actual referral source unless the arrangement has been reviewed and approved by legal counsel. Employees will report any possible violation of laws, rules, regulations, safety standards, or Company policies.

4. Coding and Billing

a. Employees are required to submit accurate and complete claims for pathology services and maintain appropriate documentation to support the claims. Employees will bill for services according to medical necessity guidelines

established by the various payors, and will notify payors of payment errors and process refunds promptly and accurately.

5. Antitrust Laws

a. Antitrust laws are created to promote free and open competition. Sharing price, cost, or profit information with our competitors or from one vendor to another is an example of a violation. Agreements to fix prices, or boycotting another competitor are illegal.

6. Fraud and Abuse Activities

a. Anti-kickback Statute

i. The federal Anti-kickback Statute prohibits the payment or receipt of anything of value that is intended to induce the recommendation of, or the actual, purchasing, leasing or ordering of any item or service that may be reimbursed, in whole or in part, under a government health care program, including Medicare or Medicaid. The Company provides certain services that may be reimbursed in whole or in part by government programs, thus, anything of value offered by the Company to induce the purchase of Company services could violate the Anti-kickback Statute. As an example, an offer of free computer equipment to a physician to attempt to induce the award of business to the Company may violate the Anti-kickback Statute. The federal government created certain "safe harbors" whereby a transaction may be structured in a certain manner to protect it from penalty under the Statute. The Company seeks to structure its business transactions in accordance with applicable safe harbors or otherwise in compliance with the Statute. In addition to the federal Anti-kickback Statute, certain states have enacted similar laws and the Company shall comply with these as well. The CCO or General Counsel will provide appropriate guidance with respect to any proposed transactions.

b. Stark Law

i. The Stark Law prohibits physician referrals for "designated health services," such as laboratory services, to any entity if the physician or an immediate family member of the physician has a "financial relationship" with the entity receiving such referral. A violation occurs regardless of the referring physician's intent in making the referral. In addition, an entity receiving a prohibited referral may not present the claim to Medicare or Medicaid for that designated health service. The Company may not accept referrals for laboratory services from a physician with whom the Company has a "financial relationship." A "financial relationship" is deemed to exist if the referring physician (or a family member of the physician) holds an ownership or investment interest in the Company or is a party to an arrangement involving any remuneration, directly or indirectly, overtly or covertly, in cash or in kind between a the physician (or his/her family member) and the Company. Thus, such a "financial relationship" may be created by a consulting agreement with a physician or the sale of goods or services to a physician. The Stark Law contains certain exceptions whereby certain arrangements are deemed not to create a "financial relationship." Such exceptions include payments made by the physician for goods or services provided at fair market value. Other exceptions may apply depending upon the circumstances, and the CCO or General Counsel will provide appropriate guidance with respect to any proposed transactions.

7. Anti-Bribery Laws

a. Foreign Corrupt Practices Act

i. The Foreign Corrupt Practices Act ("FCPA") is a federal law which prohibits any Company officer, director, employee, or agent from corruptly making, or offering to make, or authorizing the payment of, any money or anything of value, directly or indirectly, to foreign government officials in order to obtain or retain business. This prohibition includes the provision of any payment intended to influence the decision of any foreign government official in his or her official capacity, including a decision not to perform an official function. In addition to employees and officers of foreign government departments, agencies, or political parties, the term "foreign public official" may include a candidate for foreign public office and employees of state-owned enterprises or Company. The FCPA applies to payments to any foreign public official, regardless of rank or position. Companies and individuals who violate the FCPA are subject to substantial penalties, including significant fines and imprisonment.

ii. The FCPA also prohibits corrupt payments through intermediaries. Intermediaries may include joint venture partners or agents. It is unlawful to make a payment to a third party, while knowing that all or a portion of

the payment will go directly or indirectly to a foreign official. The term "knowing" can include conscious disregard and deliberate ignorance.

iii. The FCPA contains an exception for small payments made to a foreign public official necessary to secure performance of a routine governmental action, sometimes known as "facilitation payments." However, it is the Company's policy that its employees and agents shall neither make nor offer such payments.

iv. The FCPA also requires that publicly-traded companies maintain adequate financial controls over corporate assets and that transactions and dispositions of corporate assets are accurately and fairly reflected in Company records.

v. It is the Company's policy to comply with all requirements of the FCPA. The Company expects that each of its employees will conduct themselves in compliance with all applicable laws, including the FCPA and the anti-bribery laws of the countries in which the Company does business. Any questions regarding the scope of the FCPA or whether any transaction may implicate the FCPA should be directed to the CCO or General Counsel.

b. The UK Bribery Act 2010 (the UK Act) and other non-US laws

i. Other countries in which the Company does business have laws in place to criminalize bribery. Many countries, including the UK, have laws which contain extra-territorial provisions similar to the FCPA.

ii. The UK asserts extra-territorial jurisdiction over many businesses and individuals including UK-incorporated companies, UK citizens and residents as well as any business which carries on part of its business within the UK.

iii. The UK Act has provisions which are similar to the FCPA in relation to intermediaries. Facilitation payments are prohibited under the UK Act.

iv. The UK Act prohibits both active and passive public and private bribery.

v. The UK Act contains a strict liability offense of failure by a corporate organization to prevent bribery. There is a statutory defense of having in place adequate procedures designed to prevent persons associated from being involved in bribery. The definition of associated persons includes employees, intermediaries and subsidiaries and could include joint venture partners if the joint venture partner provides any services to the Company.

vi. The UK Act also contains an offense which applies to natural persons who have a close connection to the UK, who are senior managers, or who consent or connive with a corporation in relation to the corporation's involvement in bribery.

vii. The Act also contains a specific offense prohibiting the active bribery of foreign public officials.

viii. Those convicted of an offense which involves active involvement with bribery (private or public) within the European Union should expect (in addition to whatever penalty is imposed by the court that deals with the actual offence) to be excluded from participation in public sector contracts.

ix. It is the Company's policy to comply with all applicable laws prohibiting bribery which are in place in the countries in which the Company does business or seeks to do business. Any question as to what law applies in any particular circumstances or the scope of any law should be directed to the CCO or General Counsel.

x. Refer to Inform Diagnostics Policy for Anti-bribery Laws.

8. Safeguarding Company Resource

a. Employees will protect Company assets, including physical and intellectual property, and protect information against loss, theft or misuse. Employees will establish internal controls to ensure the accuracy of financial statements and all other records and reports. Employees will use Company equipment appropriately and will take measures to prevent unexpected loss of equipment, supplies, materials or services, and will obtain managerial approval for any personal use of Company equipment, supplies, materials and services. Employees will report time and attendance accurately. Employees will follow applicable intellectual property, patent, trademark, and copyright laws. Employees will adhere to the Company's Records Management policy and comply with the record retention and destruction schedule.

b. Employees will comply with all laws and regulations governing the handling, storage, use and disposal of hazardous materials, other pollutants and infectious wastes. Employees will report any possible violations of Company safety policies and procedures, laws, regulations or standards to the appropriate manager, Human Resources or Corporate Compliance Officer.

c. Company property, including computers, telephones and voice mail, software, email, and other equipment shall be used for business purposes. The Company depends upon its resources and the information that is accessed

via those resources. Much of that information is provided by means of our computer systems network and in some cases, the Internet itself. While these networks, local and worldwide, offer invaluable opportunities for sharing information and for working more efficiently, they also offer potential points of access into our Company's data, e-mail accounts, and other valuable and often confidential information. We all share a responsibility to operate our systems in a way that minimizes vulnerability to the Company.

9. Electronic Mail, Telephone & Voicemail Use & Monitoring

a. The Company recognizes each employee's need to be able to communicate efficiently with fellow employees and customers. Therefore, the Company installed an internal electronic mail (e-mail) and voice mail system to facilitate the transmittal of business- related information within the Company. All messages sent, received, composed and/or stored on these systems are Company property.

b. The Company provides an e-mail system for business purposes; however, the occasional and intermittent use of the Company's e-mail system or Internet for personal communications is generally acceptable. It is never appropriate for employees to use these tools for non-job-related solicitations, including but not limited to, religious or political causes. Employees are also prohibited from the display or transmission of sexually explicit images or messages, ethnic slurs, racial epithets or anything, which may be construed as harassing or disparaging of others.

c. Messages on the voice-mail and e-mail systems are to be accessed only by the intended recipient and by others at the direct request of the intended recipient. However, the Company may access messages on both systems at any time without cause. The existence of a password on either system is not intended to indicate that messages will remain private.

d. Employees should not rely on the erasure of messages to assume that a message has remained private. Further, the Company reserves the right to enter, search, and/or monitor the Company e-mail system and the files/transmission of any employee without advance notice, unless otherwise prohibited by law.

e. The phone system is also a way of communicating with our customers, therefore the Company reserves the right to monitor all incoming and outgoing phone calls to ensure appropriate dialog with customers as well as customer satisfaction.

10. Internet Policy

a. The following Internet policy has been adopted to ensure proper use of Company resources. It is the responsibility of all employees to adhere to this policy and to use these resources in a professional, ethical and lawful manner. Employees are given access to the Internet to assist them in the performance of their jobs.

b. Because of its global nature, users of the Internet may encounter material that is inappropriate, offensive, and, in some instances, illegal. The Company cannot control the presence of this information on the internet. Employees are personally responsible for the material they review and download from the Internet.

c. Prohibited Activities. Sending, receiving, displaying, printing, or otherwise disseminating material that is fraudulent, harassing, illegal, sexually oriented and/or explicit, obscene, intimidating, defamatory, or otherwise inconsistent with a professional office workplace is prohibited. Employees encountering such material should report it to their supervisor or Human Resources immediately.

d. Prohibited Uses. Employees may not use Company Internet resources for personal advertisements, solicitations, promotions, destructive programs (i.e., viruses and/or self-replicating code), political material, or any other unlawful use. Participation and/or postings in discussion groups, chat sessions, bulletin boards, and newsgroups are acceptable for business purposes only.

   i. Communicating Information. Employees should exercise the same or greater care in drafting e-mail, communicating in business discussion groups, and posting items to bulletin boards and newsgroups as they would for any other written communication. Anything created on the computer or Internet may, and likely will, be reviewed by others. If necessary, employees shall take steps to help protect the security of documents, including the encryption of documents.

   ii. Downloading. Computer programs and software should NEVER be downloaded from the Internet. Employees are warned that the downloading of software can cause network and computer instability, as well as security breaches that could be very damaging to the Company and/or its clients. Virus Detection. All documents downloaded from the Internet or from computers or networks that do not belong to the Company MUST be

scanned for viruses and other destructive programs before being placed onto the Company's computer system.

iii. Waiver of Privacy. The company has the right, but not the duty, to monitor any and all aspects of its computer system, including, but not limited to, monitoring sites that employees visit on the Internet, monitoring chat groups and newsgroups, reviewing material downloaded or uploaded by employees, and reviewing e-mail sent and received by employees. Employees waive any right to privacy in anything they create, store, send, or receive on their company provided computer, the Company's network, or Internet resources provided by the Company, unless otherwise prohibited by law. Compliance with Applicable Laws and Licenses. Employees must comply with all software licenses, copyrights, and all other state and federal laws governing intellectual property and on-line activity. Employees may not load any unlicensed software into any Company computers or use such unlicensed software in conducting business on behalf of Company.

11. Equal Employment Opportunity

a. The Company is an Equal Opportunity Employer. The Company does not discriminate on the basis of race, color, religion, national origin, ancestry, sex, age, military status, pregnancy, disability, sexual orientation, gender identity, participation in discrimination complaint-related activities, or any legally protected category in connection with any phase of the employment process, including, but not limited to, hiring, promotion, discharge, compensation, and benefits. Our Equal Opportunity policy also applies to all aspects of customer service. It is the policy of the Company that all customers will be treated equally and fairly without any discrimination based on race, color, religion, national origin, ancestry, sex, age, military status, pregnancy, disability, sexual orientation, gender identity, genetics, or any classifications protected by federal, state, or local law, ordinance or regulation. The Company will not tolerate such discrimination by, or directed toward, any of its employees, applicants, customers or others.

b. It is the responsibility of each employee to make certain that the working environment is free from discrimination and to report such discrimination. The Company will investigate each complaint and take all reasonable steps to prevent any form of discrimination engaged in by its employees or directed at its employees or customers.

12. Sexual and other Harassment

a. The Company is committed to providing a work environment free of unlawful harassment. Company policy prohibits any and all harassment because of race, color, religion, national origin, ancestry, sex, age, military status, pregnancy, disability, sexual orientation, gender identity, participation in discrimination complaint-related activities, or any basis protected by federal, state, or local law, ordinance or regulation.

b. The Company's anti-harassment policy applies to all persons involved in the operation of the Company and prohibits unlawful harassment by any employee of Company, including supervisors and co-workers, or by any independent contractors, and/or vendors and their employees.

c. Sexual harassment means sexual advances, requests for sexual favors, or verbal or physical conduct of a sexual nature when:

   i.submission to or rejection of such advances, requests or conduct is made either explicitly or implicitly a term or condition of employment or as a basis for employment decisions; or

   ii.such advances, requests or conduct have the purpose or effect of unreasonably interfering with an individual's work performance by creating an intimidating, hostile, humiliating or sexually offensive work environment.

d. Under these definitions, direct or implied requests by a supervisor for sexual favors in exchange for actual or promised job benefits such as favorable reviews, salary increases, promotions, increased benefits, or continued employment constitutes sexual harassment. The legal definition of sexual harassment is broad and in addition to the above examples, other sexually oriented conduct, whether it is intended or not, that is unwelcome and has the effect of creating a work place environment that is hostile, offensive, intimidating, or humiliating to male or female workers may also constitute sexual harassment. While it is not possible to list all those additional circumstances that may constitute sexual harassment, the following are some examples of conduct which if unwelcome, may constitute sexual harassment depending upon the totality of the circumstances including the severity of the conduct and its pervasiveness:

   i. Unwelcome sexual advances – whether they involve physical touching or not;

   ii. Sexual epithets, jokes, written or oral references to sexual conduct, gossip regarding one's sex life

iii. Comment on an individual's body, comment about an individual's sexual activity, deficiencies, or prowess;
iv. Displaying sexually suggestive objects, pictures, cartoons;
v. Unwelcome leering, whistling, brushing against the body, sexual gestures, suggestive or insulting comments;
vi. Inquiries into one's sexual experiences; or
vii. Discussion of one's sexual activities.

e. All employees should take special note that retaliation against an individual who has complained about sexual harassment, and retaliation against individuals for cooperating with an investigation of a sexual harassment complaint, is unlawful and will not be tolerated by the Company.
f. Other prohibited unlawful harassment includes, but is not limited to:
    i. Verbal harassment such as epithets, derogatory statements, slurs;
    ii. Physical harassment such as assault, physical interference with normal work activities;
    iii. Visual harassment such as posters, cartoons, and drawings; or
    iv. Disparate treatment based on race, color, religion, national origin, ancestry, sex, age, military status, pregnancy, disability, sexual orientation, gender identity, participation in discrimination complaint-related activities, or any other basis protected by federal, state, or local law, ordinance or regulation.
g. If any employee believes that he or she is the victim of any type of harassment, including sexual harassment or has witnessed such harassment, that employee should immediately report the incident to Human Resources or the CCO. Our Human Resources personnel and CCO are available to discuss any concerns you may have and to provide information to you about the Company's anti-harassment policy and its complaint process.
h. The Company will investigate any such report and will take whatever corrective action is deemed appropriate, including disciplining or discharging any individual who is believed to have violated this policy. The investigation will be conducted in such a way as to maintain confidentiality to the extent practicable under the circumstances. When the Company completes its investigation, it will, to the extent appropriate, inform the person filing the complaint and the person alleged to have committed the conduct of the results of the investigation.

13. Substance Abuse and Mental Awareness

a. Company employees deserve a safe environment. Thus, the Company prohibits the possession, use, sale, purchase or transfer of illegal drugs or alcohol on any of its facilities' premises, except as otherwise provided below. The Company also prohibits the consumption of alcohol on non-laboratory Company property or on Company time unless authorized by Executive Management. The Company may sponsor an event where alcohol is served on Company property during which the moderate consumption of alcohol is permitted. Individuals attending such events must still adhere to reasonable and acceptable standards of conduct. Reporting to work under the influence of alcohol or any illegal drug or possessing or selling illegal drugs while on Company premises may result in immediate termination. Drug testing may be utilized to enforce this policy. Prescription and over-the-counter drugs might also affect job performance.

14. Accuracy of Records

a. All documents, financial reports or records, which include a patient's medical information, are to be filled out in a clear manner. False or misleading wording in any record is not allowed.

15. HIPAA

a. All employees and others affiliated with the Company must respect and protect the confidential nature of protected health and other confidential information received in the course of their work for the Company. In particular, such employees must comply with state and federal laws and regulations, including the Health Insurance Portability and Accountability Act (known as "HIPAA"), governing the privacy and security of protected health information.

16. Conflicts of Interest

a. Employees will avoid conflicts or the appearance of conflicts between their own interests or an outside interest and the interests of the Company. Employees will devote their full time and ability to the Company during working

hours. Employees will also not engage in any outside activities that interfere with their ability to perform their duties to the Company properly. Employees will avoid engaging in any activity that creates an actual or apparent conflict with the interests of the Company, and will do business with individuals and entities based solely on the Company's best interests. If, in the sold judgment of the Company, a conflict of interest is found to exist, the appropriate action will be taken. Exceptions to this policy, if any, will be determined on a case-by-case basis.

17. Use of Corporate Funds and Assets

a. Employees may not use assets of the organization for their own personal benefit or gain. All property and business of the organization shall be used in a manner designed to further the Company's interests rather than the personal interest of an individual. Employees are prohibited from the unauthorized use or taking of Company equipment, supplies, software, data, intellectual property, materials or services. Further, employees are prohibited from engaging in business activities for anyone other than Company during a scheduled workday.

18. Outside Financial Interests

a. The following types of activities by individuals affiliated with or employed by Company, household members of such individuals, or a member of the individual's family, although not all-inclusive, provide examples of what may cause a conflict of interest:
   i. Any outside concern that does business with Company. This does not apply to stock or other investments held in a publicly traded corporation, provided the value of the stock or other investments does not exceed 5% of the corporation's stock. The Company may, upon a review of the relevant facts, permit ownership interests which exceed these amounts if management concludes such ownership interests will not adversely impact the Company's business interests or the judgment of the individual.
   ii. Conduct of any business not on behalf of Company, with any vendor, supplier, contractor, or agency, or any of their officers or employees.
   iii. Representation of the Company by an individual in any transaction in which he or she or a household member has a substantial personal interest.
   iv. Disclosure or use of confidential, special or inside information of or about the Company, for the personal profit or advantage of the individual or of a household or family member.
   v. Competition with the Company by an individual, directly or indirectly, in the purchase, sale or ownership of property or property rights or interests, or business investment opportunities.

19. Outside Activities

a. Employees must avoid outside employment or activities that may have a negative impact upon their job performance with Company, or that conflict with their obligations, loyalties or fiduciary responsibilities to Company.

20. Honoraria

a. Employees, with the permission of the CEO or other appropriate senior executive, may participate faculty and speakers at educational programs and functions at the request of Company. Salaried employees are prohibited from accepting honoraria without management and CCO approval.

21. Participation on Boards of Directors/Trustees

a. Employees must obtain approval from the CEO prior to serving as a member of the Board of Directors/Trustees of any organization whose interests may conflict with those of Company.
b. Employees who are asked, or who seek to serve on the Board of Directors/Trustees of any organization whose interest would not impact Company (for example, civic, charitable, fraternal and so forth) are not required to obtain such prior approval.
c. All fees/compensation (other than reimbursement for expenses arising from Board participation) that are received for Board services provided during normal work time shall be paid directly to Company.
d. Employees who are required to submit an annual Conflict of Interest disclosure statement must disclose all Board of Directors/Trustees activities in that statement unless those activities did not require prior approval as described above.

e. The Company retains the right to prohibit membership on any Board of Directors/Trustees where the Company decides such membership might conflict with the best interest of Company.

22. Gifts

a. Gifts are not appropriate if offered, given or accepted in exchange for, or as a reward or inducement for, business. Most importantly, employees shall not knowingly or willfully offer, pay, solicit or receive anything of value from a potential or actual referral source (e.g., physicians and hospitals) to induce the referral of business reimbursable by Medicare, Medicaid, or any other federal or state health care program.
b. As a general matter gifts are discouraged. However, if gifts are proposed or offered, in order to help avoid both the reality and the appearance of improper relations with past, current, potential or future vendors, suppliers, contractors, or providers, the following guidelines apply to the offering, giving and receiving of gifts by employees.
c. Employees may not accept gifts or anything else of value that might reasonably be considered to affect an individual employee's judgment in carrying out any duties on the Company's behalf.
d. Employees, may however, accept small gifts of nominal value (up to $25.00 per gift or $50.00 annually). Solicitation of money, non-money gifts, gratuities, or any other personal benefit or favor of any kind from vendors, suppliers, contractors, or patients is prohibited.
e. All employees must report to the Corporate Compliance Officer the acceptance of any gifts that exceed the per-gift and/or the annual limit.
    i. Refer to the Companies Policy on Gifts, Meals, and Entertainment.

23. Reporting Obligation and Helpline Information

a. Employees who have knowledge of actual or possible wrongdoing, misconduct or violations of the Company's Code, compliance policies and procedures, or the laws, rules and regulations by which Company is governed, must immediately report the matter to either
    i. the department member of their senior management team;
    ii. a Human Resource Representative;
    iii. the Corporate Compliance Officer – John Rasmussen;
    iv. or the EthicsPoint Report System. Reporting via the EthicsPoint Report System can be done via the Internet at www.ethicspoint.com, by calling toll-free (888) 493-1869, or by contacting the CCO.
b. EthicsPoint is an anonymous and confidential reporting tool to communicate misconduct and promote a positive work environment. EthicsPoint is carefully designed to maintain confidentiality and anonymity at every step. No reporter will be required to disclose his or her identity and no attempt will be made to trace the source of the identity of the reporter when anonymity is requested. If the reporter has revealed his or her identity, confidentiality will be maintained to the extent practicable and allowed by law. Reporters should be aware, however, that it may not be possible to preserve anonymity if they identify themselves, provide other information which identifies them, if the investigation reveals their identity, or if they inform people that they have called the EthicsPoint reporting system. Reporters should be aware that the Company is legally required to report certain types of crimes or potential crimes and infractions to external agencies.
c. Retaliation against an employee who has reported a violation of the Code, Company policies and procedures, law, or applicable regulations is strictly prohibited by Company policy and will not be tolerated.

Use of Computer Systems Policy

1. Purpose

a. The purpose of this policy is to outline the acceptable use of computer equipment at Inform Diagnostics. These rules are in place to protect the employee and Inform Diagnostics. Inappropriate use exposes the Company to risks including virus attacks, compromise of network systems and services, and legal issues.

b. The computers, network, Internet connections, software applications and electronic mail systems (collectively referred to as "computer systems") made available to Users shall be used for business purposes.
c. Refer to the Inform Diagnostics Code of Conduct regarding the proper use of Company property available to you as a Inform Diagnostics employee.

2. Special Situations

a. Confidential Information: The Inform Diagnostics information system includes confidential information, including proprietary information, personnel records, and individually identifiable health information. Inform Diagnostics has a legal and ethical obligation to safeguard the privacy of that information. Refer to the Inform Diagnostics Code of Conduct regarding safeguarding Company resources available to you as a Inform Diagnostics employee.

3. Scope

a. These policies apply to all persons who use the computer systems of Inform Diagnostics, including employees, contractors, students and volunteers. This policy applies to all equipment that is owned or leased by Inform Diagnostics and accesses the Company Network.

4. Definitions

a. Computer Systems - Computers, network, Internet connections, software applications and electronic mail systems made available to Users.
b. Software Piracy - The unauthorized copying or distribution of copyrighted software. This can be done by copying, downloading, sharing, selling, or installing multiple copies onto work computers (e.g., music, Microsoft Suite, Adobe products).
c. Users - All persons who use the computer systems of Inform Diagnostics, including employees, contractors, students and volunteers.
d. Sensitive Information - Information or knowledge which if disclosed to or accessed by unauthorized persons could adversely affect Inform Diagnostics, its employees, programs, or participants served by its programs. Such information or knowledge includes but is not limited to routine business information, confidential information, private health information as set forth by HIPAA, and personal information.
e. Protected Health Information (PHI) - All individually identifiable health information held or transmitted, in any form or media, whether electronic, paper, or oral.
f. Personal Information (PI) - First name and last name or first initial and last name of an individual in combination with one of the following: Social Security number, credit card or debit card, financial account number, other account number (such as health insurance).
g. Encryption - A procedure used to convert data from its original form to a format that is unreadable and/or unusable to anyone without the tools/information needed to reverse the encryption process.

5. Policy

a. Software Licensing and Piracy
   i. Software piracy is the unauthorized copying or distribution of copyrighted software. This can be done by copying, downloading, sharing, selling, or installing multiple copies onto personal or work computers. What a lot of people don't realize or don't think about is that when you purchase software, you are actually purchasing a license to use it, not the actual software. That license is what tells you how many times you can install the software, so it's important to read it. If you make more copies of the software than the license permits, you are stealing.
   ii. Inform Diagnostics will determine the hardware and software to be installed on each workstation, including portable computers. Users are not permitted to install additional hardware or software without the permission of the IT department. This includes free software or shareware downloaded from the Internet or personally owned hardware or software. The protection of the employees and Inform Diagnostics all systems owned by Inform Diagnostics must only have Inform Diagnostics licensed software and hardware (no home/ personal software can be used for business use).
   iii. Refer to the Inform Diagnostics Code of Conduct regarding the compliance with applicable software laws and licenses as a Inform Diagnostics employee.

6. **Use of Computer System**
   a. Users will be authorized to access our computer system and records stored on that system to the extent necessary to enable them to perform their work.
   b. By logging-into Inform Diagnostics system I agree to all of the following:
      i. That the user account issued to me is a unique code that gives me authorized access to the systems and applications of the institution licensing the same ("Licensee"),
      ii. That any information accessed is strictly confidential and to be used only in the performance of my necessary
      iii. duties,
      To abide by all policies and procedures adopted by Licensee as well as all current federal and state laws governing information technology and personal information and patient confidentiality and such access, including the Health Insurance Portability and Accountability Act (known as "HIPAA"), which governs the privacy and security of protected health information, and to use appropriate safeguards to protect confidential patient information and personal information and make no disclosures except as required by law or for the purposes of my necessary duties.
      iv. That if at any time I feel the confidentiality of my security user account/password has been compromised, I will immediately contact the appropriate Compliance Officer at my Licensee institution and participate in investigating the circumstances around the compromise, and
      v. That if I abuse access privileges, I may be subject to disciplinary action including but not limited to termination, civil penalties and criminal penalties."
      vi. The Company reserves the right to monitor any and all aspects of its computer system. Employees waive any right to privacy in anything they create, store, send or receive on their company provided computer, the Company's network, or Internet resources provided by the Company, unless otherwise prohibited by law.

7. **Authentication of User Identity**
   a. Each person authorized to use our computer systems will be issued a user identity. User identities are confidential, and should not be shared with other people.
   b. When Users log onto our computer system, they will be asked to enter a User Identity.

8. **Passwords and Password Management**
   a. Each authorized User will be issued a temporary password. The first time a User logs into the company network, he or she will be asked to change their password to one he or she creates.
   b. Users are expected to follow these password complexity guidelines when creating passwords:
      i. Passwords must be at least 8 characters in length.
      ii. Mix letters, numbers and symbols if possible.
      iii. The last 5 passwords are remembered and cannot be repeated.
      iv. Avoid use of words.
      v. Avoid use of names of family members, pets, favorite sports teams or other obvious passwords.
      vi. Never use the word "password" as your password. Consider use of a Passphrase. Make up a sentence and then use the first letter of each word in the sentence to create your password. For example: *Next Winter I'm Going To Hawaii & Surf* = NWIGTH&S Passwords are confidential.
      vii. They should not be shared with other people.
      viii. Passwords should not be written down and left in obvious places, such as under a keyboard or a "sticky" note on a monitor. Passwords must be changed every 90 days.

9. **Authorized Access**
   a. The Inform Diagnostics computer system will not allow users whose identity and right of access cannot be authenticated. Users who have difficulty logging onto the computer system should report the problem to the IT Help Desk (214-596-7443, helpdesk@InformDx.com).

10. Access Control

a. Permission for individual access to protected health information or personal information will be based on the work each person performs and the records the person needs to perform that work. An individual's user identity and password will determine their access to records.

11. Workstation Use

a. Inform Diagnostics will determine the hardware and software to be installed on each workstation, including portable computers. Users are not permitted to install additional hardware or software without the permission of the system administrator. This includes free software or shareware downloaded from the Internet.

12. Patches

a. The information system department of Inform Diagnostics will download and install patches to update operating system and application software and reduce security risks.

13. Protection against Malicious Software

a. All computers used by Inform Diagnostics are protected against malicious software, including computer viruses. Trojan horses, spyware, etc. All anti-virus software definitions must be kept current.
b. Disabling or modifying antivirus software for any reason without permission of the Information Technology Department is strictly prohibited. Users will ensure that any personal computers that are used to remotely connect to the Company network are configured with approved antivirus software.
c. Please refer to Anti-Virus Procedures for more details.

14. Firewalls

a. The Inform Diagnostics computer system includes firewalls and intrusion detection software to prevent access by unauthorized persons. Inform Diagnostics issued portable computers must have firewalls enabled.

15. Reporting Security Incidents

a. Users must report any suspicious, unauthorized or malicious activity that might affect the security of the computer system or the confidentiality, availability or integrity of confidential information to the Corporate Security (security@InformDx.com) and the IT Help Desk (214-596-7443, helpdesk@InformDx.com) as soon as it is discovered.

16. Disposal of Electronic Media

a. If a User wishes to dispose of any CD-R, CD-RW, tape, USB flash drive, or other electronic media used to store Company information, the User should notify the IT Help Desk (214-596-7443, helpdesk@InformDx.com). The storage devices of any such electronic media must be either physically destroyed or "wiped clean".

17. Electronic Mail Policy

a. Users have an obligation to use e-mail appropriately, effectively, and efficiently. Refer to the Inform Diagnostics Code of Conduct regarding the proper use of electronic mail available to you as a Inform Diagnostics employee.
b. Users should not share their electronic mail identity and password with anyone else.
c. Electronic mail can be forwarded, intercepted, printed and stored by others. Users must use even greater discretion with regard to the information that they include in electronic mail than they apply to written documents.
d. Employees are prohibited to use a personal email account (e.g. AOL, Gmail, Hotmail, etc.) for the sending or receiving of email relating to Inform Diagnostics business.
e. Any electronic mail message that includes confidential information should include a subject header or "flag" to indicate that the communication is personal and confidential. There shall be no identifying information in the subject line of the message.
f. Refer to the Inform Diagnostics Policy on Confidentiality and General Uses and Disclosure of Protected Health Information.
g. All messages originated or transported within or received into Inform Diagnostics electronic mail system are the property of Inform Diagnostics.

h. The Company reserves the right to monitor any and all aspects of its computer system. Employees waive any right to privacy in anything they create, store, send or receive on their company provided computer, the Company's network, or Internet resources provided by the Company, unless otherwise prohibited by law.
i. Sensitive patient data, Personal Information (PI) and Protected Health Information (PHI) should only be sent by e-mail within the Inform Diagnostics network. This type of information should not be communicated outside of the Inform Diagnostics network via unprotected e-mail; communicating confidential information (patient treatment, client billing, etc.) in this manner presents a significant risk of disclosure because e-mail is not encrypted.
j. Any electronic mail from Inform Diagnostics that includes protected health information will be labeled "CONFIDENTIAL CONTAINS PHI" at the beginning and end of a message. Refer to the Inform Diagnostics Policy on Confidentiality and General Uses and Disclosure of Protected Health Information.

18. Web-based email

a. Web e-mail allows employees a convenient method to access Inform Diagnostics email through a web browser when they are away from the office. Although web-email access requires a Inform Diagnostics logon ID and password, employees are also responsible for proper handling and protection of sensitive information on all email and attachments to reduce the likelihood of inadvertent data leakage.
b. Email and attachments should not be downloaded to non Inform Diagnostics equipment from web-based email away from the office. Email and attachments should not be sent to or printed on non Inform Diagnostics approved printers away.

19. Internet Access

a. Users may access the Internet through Inform Diagnostics' network. Refer to the Inform Diagnostics Code of Conduct regarding the proper use of the Internet available to you as a Inform Diagnostics employee.

20. Remote Access Policy

a. The "always on" nature of external broadband Internet services can leave PCs open to intrusion and could put the company network and sensitive information at risk. In order to prevent hackers from potentially hijacking a Virtual Private Network (VPN) session for use as an entryway to internal corporate resources, it is critical that Inform Diagnostics controls VPN access.
b. Inform Diagnostics will allow specified Users the right to access the computer system from remote locations. Remote access rights must be approved by User's supervisor and IT.
c. In order to ensure the security of our computer system and safeguard confidential information, the following policies apply:
    i. Access to the Inform Diagnostics computer system from outside of its defined network perimeter must be controlled by Virtual Private Network (VPN) technology in accordance with organization Security Policies. The IT Help Desk will work with persons authorized to access the system remotely to set up a VPN.
    ii. Remote access from non-Inform Diagnostics personal computers is prohibited. VPN software will only be installed on company-issued portable computers.
    iii. VPN access will be granted to employees based on job responsibilities.

21. Portable computing devices

a. A wide variety of third parties have entrusted their information to Inform Diagnostics for business purposes, and all employees must do their best to safeguard the privacy and security of this information. Client and patient data is accordingly confidential and access will be strictly limited based on business need for access.
b. Portable computing devices (e.g., laptop computers, smart phones, cell phones) and removable media (e.g., flash memory devices, removable hard drives) that could provide access to confidential information should be kept under careful control.
c. Unattended portable computing devices must be physically secure. This means they must be locked in an office, locked in a desk drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system.
d. Portable computing devices should be kept in employees' personal possession when in public places (e.g., airports, restaurants).
e. Do not treat them as "checked baggage" (e.g., on trains, airplanes, etc.); keep them with you while traveling.
f. Place them into a locked suitcase when leaving them in a hotel room or other only semi-private location.
g. Do not leave device in your car.

h. Exit all programs when the device is not in use.

22. Removable Media

a. Removable Media includes devices that are readable and/or writeable by the end user and are able to be moved from computer to computer without modification to the computer. This includes flash memory devices such as USB drives, cameras, MP3 players and PDAs; removable hard drives; optical disks such as CD and DVD disks; floppy disks and any commercial music and software disks not provided by Inform Diagnostics.
b. Saving PI and PHI on removable media presents a privacy risk and is prohibited.
c. All company-issued computers will be configured with antivirus protection to prevent viruses from spreading through removable drives. When an USB device is inserted into a computer, this software will automatically scan it and block and delete detected viruses.

23. End User Computing

a. Applications developed by end-users (usually through the use of desktop tools such as Microsoft Excel, Microsoft Word, and Microsoft Access) are not supported by IT. For this reason, these tools require enhanced control focus from the developer (end-user). Guidance for how to protect and validate End User Computing files:
   i. Backups: Data that needs to be backed up should be stored on an IT Department authorized server. Users are responsible for backing up any data stored elsewhere, including data on their desktop. This will ensure that critical information, including key spreadsheets, can be recovered in the loss of data or other crisis.
   ii. Access Control: Access to critical spreadsheets, databases and associated queries can be limited at the directory level by saving files on a central server and assigning authorization rights. Requests for new folders and restricting access to folders should be sent to the Help Desk at helpdesk@InformDx.com.
   iii. Password Protect Key Documents: Spreadsheets and Word documents can also be password protected to restrict access. File password protection procedures in Microsoft Office 2007 are listed below:
      (1) Click the Microsoft Office Button, point to Prepare, and then click Encrypt Document.
      (2) In the Password box, type a password, and then click OK.
      (3) In the Reenter password box, type the password again, and then click OK.
      (4) To save the password, save the file.

24. Password Protect Worksheet Elements

a. In addition to residing under restricted access and password protected files, critical data fields should be safeguarded against accidental or inappropriate changes and deletions. Cells or queries that include sensitive or complex calculations can be locked. Instructions for this procedure are located in the Microsoft help guide under "security and privacy".
b. Prohibited Uses of Inform Diagnostics Computer System
c. Refer to the Inform Diagnostics Code of Conduct regarding the prohibited activities and uses of the Internet and Company property available to you as a Inform Diagnostics employee.

25. Exceptions

a. Implementation not Practicable: In any situation where this policy cannot be applied, the circumstances and compensating measures should be documented using the Request for Exception form and approved by the IT Governance Oversight Committee. It is the responsibility of the IT Department to maintain this documentation for audit purposes.
b. Reference/Policies/Procedures/Forms
   i. Inform Diagnostics Code of Conduct
   ii. Portable Computing Security Policy
   iii. Policy on Confidentiality

26. VIOLATION CONSEQUENCES

a. Employees of Inform Diagnostics who violate any part of this policy may be subject to disciplinary action as outlined in the employee handbook.
b. Inform Diagnostics reserves the right to immediately terminate for cause any contract or business relationship with any non- employee who violates any part of this policy.

c. Refer to the Inform Diagnostics Code of Conduct regarding the obligation that you have as a Inform Diagnostics employee for reporting wrongdoing, misconduct or violations of the Company's Code, compliance policies and procedures, or the laws, rules and regulations by which the Company is governed.

Nondisclosure Agreement

This Nondisclosure Agreement ("the Agreement") is made and entered into on the last signature date (the "Effective Date") by and between you ("Employee") and Inform Diagnostics, Inc., including and on behalf of its affiliates ("Company"). Employee or Company may be referred to individually as a "Party," and collectively the "Parties" in this Agreement.

In consideration of the disclosure and receipt of Confidential Information (as defined below) and in order to protect said information and thereby preserve the business, assets and goodwill of the disclosing party, the Parties hereto agree as follows:

1. **Definitions:** Each Party disclosing Confidential Information ("Discloser") and receiving such Confidential Information ("Recipient") shall act in accordance with the terms and conditions of this Agreement in order to protect each other's Confidential Information from unauthorized use or disclosure. The term "affiliates" as used in this Agreement means any corporation, Limited Liability Company, partnership, trust, joint venture or other such entity that is controlled by, controlling, or under common control with a Party. "Control" means: (i) the enjoyment of direct or indirect beneficial ownership of at least fifty (50%) interest in the outstanding voting stock (or the equivalent) of the company (or other entity), or (ii) having the right to direct, appoint or remove a majority of members of its board of directors (or their equivalents), or (iii) otherwise having the power to direct the general management and operations of the company or other entity, by law or contract.

2. **Description of Confidential Information:** The confidential and proprietary information that is the subject of this Agreement is described as follows: any information (a) designated as "confidential" or "proprietary" (or the like) either orally or in writing by the Discloser, (b) not generally known by non-Discloser personnel (other than persons subject to confidentiality obligations), and (c) relating to the Company's business, including, without limitation, patents (including patent applications and patent rights), copyrights, trade or service marks, trade secrets, inventions (whether or not patentable), discoveries, know-how, methods, technology, computer programs or software (including source code), databases, products, research materials or data, works of authorship, compounds or materials (including cell lines, tissues, samples or molecules), the existence of this Agreement and its terms and the fact that Employee is evaluating the Company's confidential information, including the Company's interest in the development of the New Proprietary Laboratory Information System and any of its related components or information about or pertaining to the Company's commercial relationships (including but not limited to supplier names, business partner information, customer names and related information), marketing and development, strategy, personnel, operations, pricing and pricing policies, and financial condition and performance (collectively "Confidential Information"). With regard to oral disclosures, such will be follow-up within a reasonable period of time by the Discloser and as applicable given the nature of the oral disclosure:
(d) either reducing the same in its entirety to tangible form, or (e) providing a written summary within 10 days after the initial disclosure, referencing the same and reminding the Recipient of the "confidential" or "proprietary" nature thereof.

3. **Use of Confidential Information:** Recipient agrees not to use the Company's Confidential Information for any purpose except the following: Discussions relating to the New Proprietary Laboratory Information System and any of its related components. Each Party, in its sole discretion, may choose whether or not to exchange its Confidential Information with respect to any discussions or evaluations related to this Agreement.

4. **Privilege; Legal Proceedings:** To the extent that any Confidential Information includes materials that are or may be subject to attorney-client privilege, work product doctrine or any other applicable evidentiary privilege concerning pending or threatened legal proceedings or governmental investigation, the Parties acknowledge and agree that they have a commonality of interest with respect to such matters; and it is each Party's intention and mutual understanding that the sharing of such Confidential Information by either Party, is not intended to, and will not waive or diminish in

any way the confidential and privileged nature. All Confidential Information that is entitled to protection under attorney-client privilege, work product doctrine or other applicable privilege will remain entitled to such protection under these evidentiary privileges, under this Agreement and/or under the joint defense doctrine.

5. **Non-Disclosure:** Except where the discloser has given its prior written consent, the Recipient and its Representatives will not share with any third party any of the Discloser's Confidential Information. In addition, "Confidential Information" shall include the fact that Confidential Information has been made available to the other Party, that discussions are taking place concerning a possible business relationship between the Parties, and any of the terms, conditions or other facts with respect to such discussions, including the status thereof. Employee shall not file any patent application(s) containing or based, in whole or in part, on any of the Company's Confidential Information and/or relating to the New Proprietary Laboratory Information System and any of its related component.

6. **Feedback:** Any ideas, suggestions, guidance or other information disclosed by Employee related to the Company's Confidential Information and any intellectual property rights relating to the foregoing shall be collectively deemed "Feedback." Inform Diagnostics shall own all Feedback, and Recipient agrees to assign and hereby assigns to the Company a nonexclusive, perpetual, irrevocable, royalty fee, worldwide license (with the right to grant and authorize sublicenses) to make, have made, use, import, offer for sale, sell, reproduce, distribute, modify, adapt, prepare derivative works of, display, perform and otherwise exploit such Feedback without restriction.

7. **Confidentiality Period:** This Agreement, once executed by the last Party to sign, shall be valid for a period of one (1) year commencing on the Effective Date and continuing thereafter until expiration or termination of employment. Each Party's obligations as set forth in this Agreement with respect to the protection, use and non-disclosure of the other Party's Confidential Information shall survive and remain in full force and effect for a period of five (5) years following such expiration or termination.

8. **Standard of Care:** Recipient shall protect the Discloser's Confidential Information to prevent the unauthorized use, dissemination, or publication thereof, using the same degree of care (but no less than reasonable care), as Recipient uses to protect its own Confidential Information of a like nature. In accordance with this Agreement, Recipient shall take all reasonable measures (a) to protect the secrecy of and avoid disclosure or unauthorized use of disclosed Confidential Information, and (b) to prevent such Confidential Information from falling into the public domain or the possession of persons other than those persons authorized by this Agreement to have such information. Each Recipient agrees to promptly notify the Discloser in writing of any misuse or misappropriation of the Discloser's Confidential Information of which Recipient becomes aware.

9. **Return of Property**: At any time upon the request of the Company, the Recipient shall promptly return to the other any Confidential Information that has been furnished hereunder, along with all hard or electronic copies thereof. Alternately, the Company may request the Recipient destroy any or all Confidential Information, and all hard or electronic copies thereof. The Company may request the Recipient provide written certification as to the return or destruction, in accordance with this paragraph, and the Recipient will promptly provide such certification.

10. **Exclusions from Definition of Confidential Information**
    a. For avoidance of doubt, this Agreement imposes no obligation upon Recipient with respect to information that:
        i. was in Recipient's possession without a duty of confidentiality before receipt from Discloser;
        ii. is or becomes a matter of public knowledge through no fault of Recipient;
        iii. is rightfully received by Recipient from a third party without a duty of confidentiality;
        iv. is disclosed by Discloser to a third party without a duty of confidentiality on the third party; I is independently developed by Recipient without use of the Confidential Information; or
        v. is disclosed by Recipient with Discloser's prior written approval. Notwithstanding any other provision of this Agreement, disclosure of Confidential Information shall not be prohibited to the extent required to comply with applicable laws or regulations, or with a valid court or administrative order, provided that Recipient:
        vi. promptly notifies Discloser in writing of the existence, terms and circumstances of such required disclosure;
        vii. consults with Discloser on the advisability of taking legally available steps to resist or narrow such disclosure; and

viii. takes all reasonable and lawful actions to obtain confidential treatment for such disclosure.

11. Warranty

a. Each Discloser warrants that it has the right to make the disclosures under this Agreement. EXCEPT AS DESCRIBED IN THIS AGREEMENT, NO OTHER WARRANTIES ARE MADE BY EITHER PARTY. ANY INFORMATION EXCHANGED UNDER THIS AGREEMENT IS PROVIDED "AS IS."

12. No Rights

a. This Agreement does not grant or confer, expressly or impliedly, to either Party any intellectual property rights, whether by ownership interest or license, in the other Party's Confidential Information, except for the limited rights to use Confidential Information as necessary to carry out the purposes set forth in Section 3 above.

13. Disclosure to Representatives:

a. Each Party agrees that the other Party may disclose any of the Confidential Information to its own corporate affiliates as well as to the directors, officers, employees, subcontractors, agents or advisors (including, without limitation, attorneys, accountants, consultants, bankers and financial advisors) (collectively, "Representatives") who need to know such information for the sole purpose described in Section 3 of this Agreement and who are under obligations of confidentiality no less restrictive than the terms contained in this Agreement. Each Party will be responsible for any material breach of this Agreement by any of its Representatives.

14. Injunctive and Other Relief

a. It is understood and agreed that Disclosing Party would be irreparably injured by a breach of this agreement by Recipient; that money damages would not be an adequate remedy for any such breach; and that Disclosing Party shall be entitled to equitable relief, including injunctive relief and specific performance, as a remedy for any such breach, which shall be entitled to reasonable attorneys' fees and other costs reasonably incurred to remedy any and all breaches of this Agreement by Recipient. In the event of a breach or threatened breach of this Agreement, the injured Party may immediately seek injunctive relief in any court of competent jurisdiction. The Recipient shall mitigate, to the extent practicable, any harmful effects of any unauthorized use or disclosure of the other Party's Confidential Information in violation of the terms of this Agreement.

15. Miscellaneous

a. This Agreement imposes no obligation on either Party to enter into any other transaction or commitment, or purchase, sell, license, transfer or otherwise dispose of or acquire any technology, services or products of the other Party.
b. Except as to the sale or transfer of a Party's business or substantially all of the assets to which this Agreement relates, this Agreement may not be assigned by either Party. This Agreement shall be binding upon and inure to the benefit of the Parties and their permitted successors and assigns.
c. This Agreement may be executed in counterparts, including facsimile or electronic copies, which taken together shall constitute one and the same agreement.
d. Both Parties shall adhere to all applicable laws, regulations and rules relating to the export of technical data, and shall not export or re-export any technical data, any products received from Discloser, or the direct product of such technical data to any proscribed country listed in such applicable laws, regulations and rules unless properly authorized.
e. This Agreement does not create any agency, partnership or joint venture relationship.
f. All additions or modifications to this Agreement must be made in writing and must be signed by both Parties. Any failure to enforce any provision of this Agreement shall not constitute a waiver thereof or of any other provision hereof.
g. The Parties agree that this Agreement shall be governed by and construed in accordance with the laws of the State of Texas, without regard to its choice of law provisions.

Business Driver Policy

This policy applies to Inform Diagnostics employees and contractors, who are deemed ***Drivers*** for the Company, to communicate Driver guidelines regarding usage, safety, and accident procedures.

1. DEFINITIONS

a. Acceptable Driver Status - MVR evaluation determined to be acceptable and Driver status is not affected.
b. Driver - The term "Driver" shall apply to the Company employees and contractors, who travel for Company business 50% or more as part of their routine job responsibilities.
c. Motor Vehicle Report (MVR) - A report provided by the Department of Motor Vehicles (DMV) that includes, but is not limited to, driving history, driver's license status, traffic accidents, driving record, convictions and fines, and DUI public records.
d. Unacceptable Driver Status - DMV evaluation determined to be unacceptable by the Company. Reasons may include an unsatisfactory DMV report or a Driver who is considered to be in violation of the intent of this policy, may result in a loss of the privilege of driving for Company business, and may include termination of employment.
e. Vehicle - For purposes of this policy, the term "vehicle" represents a personal motor vehicle while on Company business, or a rental vehicle while on company business.

2. DRIVER COMPLIANCE

a. HR will run and evaluate Motor Vehicle reports for all Drivers annually.

3. DRIVER CRITERIA & ADMINISTRATION

a. Role must be qualified as a "Driver" for the Company.
b. Driver must have a valid, current driver's license.
c. Driver license restrictions: The Company will recognize a temporary restricted license to use for work as ordered by the jurisdiction.
d. Drivers must acknowledged they have read and agreed to abide by the Business Driver Policy.
e. Ensure any changes to driver's licenses (name, address, state, etc.) are changed in the HR System.
f. New Drivers for the company (Including external hires and current employees moving into driving roles for the first time) will have MVR's run and evaluated by HR, prior to starting in the role. f. Insurance minimum coverage requirements: $100,000 Liability.
    i. Damage to vehicles, as well as injury to family members, friends, etc., will not be covered by the corporate coverage and therefore, is the sole responsibility of the Driver.
g. Maintain state vehicle inspections where required by law.
h. Maintain vehicle in a safe operating condition.
i. Drive in a safe, responsible manner, while maintaining a good driving record.

4. DRIVER SAFETY REQUIREMENTS

a. Comply with state laws.
b. If legal, phone usage while driving should be kept to a minimum. Complete calls while parked and/or use the phone in a "hands free" mode. Safety should always take precedence over conducting business.
c. No texting or emailing while driving.
d. No operating a vehicle when impaired (including by illness, fatigue, injury, prescription medication, or other reasons).
e. Both Drivers and passengers must wear seatbelts at all times.
f. Only authorized personnel should ride in vehicles while being used for Company business.
g. Always drive defensively to reduce your risk behind the wheel.
h. No radar detectors may be used while vehicle is being used for Company business.
i. While unattended, vehicles must remain locked.

5. ACCIDENT PROCEDURES

a. Accidents, regardless of severity, must be reported to the police of jurisdiction, and HRhelpline@InformDx.com within 24 hours of occurrence and Driver must provide a copy of the police report when available.

b. Record names, addresses, and contact information of the other driver(s), witnesses, and occupants of the other vehicles, and any medical personnel who may arrive at the scene. Provide the other party the appropriate information as well.
c. Notifying your auto insurance carrier regarding any ensuing claims.
d. Do not discuss the accident with anyone except the police while at the scene. Allow police to determine liability for the accident.
e. In the event a law suit is filed naming Inform Diagnostics, immediately forward a copy of all documents to our legal department.
f. Drivers are responsible for insurance deductible. Deductibles are not eligible for reimbursement.

2. SUSPENSION OF DRIVING PRIVILEGES

a. Unsatisfactory DMV report, or a Driver who is considered to be in violation of the intent of this policy, may result in a loss of the privilege of driving any vehicle for Company business, and may include termination of employment.
b. Suspension of the Company driving privileges may last for a period of 6 months, unless the violation is no longer valid. The suspension begins at the date of legal conviction or the Company imposed sanction.
c. Drivers whose license is revoked or suspended for any reason are required to immediately notify HR via the HRhelpline@InformDx.com, as well and their manager. They must immediately discontinue driving any vehicle for business reasons. Failure to do so may result in disciplinary action, up to and including termination of employment.

3. COMPLIANCE TO POLICY

a. This policy shall be part of the Company's business practices and compliance program. This program is not limited to falsifying the Company documents or records, engaging in acts of dishonesty, fraud or theft and unauthorized use of the Company property.
b. The Company has developed controls for protection against financial and legal risk through this policy and it will be strictly enforced. If you believe this policy or any other has been violated, please contact the Company's Ethics Point Hotline or the Compliance Officer, immediately. If there has been a failure to follow this policy, the situation will be documented and forwarded to all appropriate departments, which may include, but is not limited to:
    i. Executive Management
    ii. Legal
    iii. Human Resources
c. Disciplinary action up to and including termination may result.

4. RELATED INFORMATION

a. Fixed and Variable Rate (FAVR) Program Policy
b. Travel and Expense Policy