	Intermountain Forensics	SOP #	ADM-117
		Revision #	02
Forensic DNA Technical Leader Approval		Issue Date	
		03/13/2023	

Confidentiality

1. Purpose

This document describes the overall confidentiality policy of the laboratory.

2. Summary

The policy in this document describes the confidentiality of the laboratory to ensure absolute confidence in unbiased and confidential laboratory processes and management of data and personally identifiable information.

3. Procedure

1. Intermountain Forensics will maintain STRICT confidentiality of all information pertaining to a client, the client's case, the client's samples, testing plan and status, financial information, submission status and any client/case information and/or documents relayed by the client to Intermountain Forensics. Violation of IMF's Confidentiality policy shall subject principals, employees, and agents to disciplinary action, up to and including termination or legal action.
2. Confidential information shall only be duplicated for internal use and shall be disposed of in accordance with IMF's document retention policy.
3. The CEO, presently a licensed attorney, regularly reviews DNA-related rules, regulations, and court decisions that may impact the laboratory's obligations on dissemination of or access to confidential information provided to Intermountain Forensics.
4. Access to Customer Information
    a. Electronic Access
        i. All case-related documents, case files, and reports are housed on a secure cloud-based server using Microsoft Azure. The server may only be accessed by a restricted number of individuals maintained by the laboratory director (or designee). Network security is multi-level, always updated by the hosted solution, and far more robust than traditional servers.
        ii. Access to JusticeTrax and other electronic client data is restricted to Laboratory personnel.
            1. All Laboratory personnel must have executed confidentiality/ nondisclosure agreements prior to the access being granted.
    b. Physical Access
        i. Only authorized individuals have physical access to the laboratory. Authorization must be obtained from a member of executive management prior to access being granted.
            1. Before allowing persons physical access to the laboratory, Intermountain Forensics personnel ensure that no confidential information is visible.
            2. Intermountain Forensics requires immediate retrieval of any items printed, and of shredding all confidential printed material immediately when no longer needed. Electronic data is maintained indefinitely.
        ii. Intermountain Forensics utilizes an electronic security system that records all visits to the laboratory, including all areas to which visitors are permitted access.

iii. Further detail on physical access is in ADM-101 Facilities and Security

c. Access Approval
   i. Client information is only available to Executive Management and other laboratory personnel such as DNA analysts and molecular biologists.
      1. As a requisite to employment, and/or volunteer work for or with the laboratory, employees/volunteers are required to sign NDA/Confidentiality agreements
   ii. Client information is not available to the CEO or Board of Directors. The CEO may learn the identity of clients and general information regarding the type or amount of work expected to be associated with clients, solely as needed for management or planning purposes.
      1. The CEO has executed a confidentiality/nondisclosure agreement.
   iii. The Intermountain Forensics Executive Director has access to client information solely to the extent necessary for billing and related administrative purposes.
      1. The Executive Director has executed a confidentiality/nondisclosure agreement.
   iv. Non-Intermountain Forensics personnel do not have open access to client data, but other personnel, including volunteers, are routinely asked to execute confidentiality/nondisclosure agreements, in the event they are provided limited access to information pertaining to a client, the client's case, the client's samples, testing plan and status, financial information, submission status and any client/case information and/or documents relayed by the client to Intermountain Forensics

5. Dissemination of Information to Third Parties
   a. Requests to information to individuals outside of the client's agency will only be fulfilled upon informed, written, reasonably time-limited consent from the customer or proof of authority or legal compulsion, such as a court order or subpoena.
      i. Written permission from the customer may be in the form of email. However, the email must have been received from a known or confirmed email address which has been previously provided by the customer.
         1. Documentation of the written permission or notification (in the event of a legal compulsion) must be saved in the case file.
         2. In the case the client is an unemancipated minor, the minor and the parent or guardian or in the case of legal incapacity, a court-appointed guardian are the individuals must be solicited for permission, unless the minor or person with a legally appointed guardian is permitted by law to receive services without the parent's or guardian's consent, so the minor or person with a guardian may release information without additional consent.
      ii. If any Intermountain Forensics personnel require clarification on the extent of permissible disclosure, they should clarify with the agency and obtained clarification in writing before sharing information with another entity.
   b. Executive Management must be notified in writing at the time a release of information request is received. The written communication is to be saved in the case file after approval to proceed with dissemination is received.
   c. Intermountain Forensics may share non-personally identifying data in the aggregate regarding services to their clients and non-personally identifying demographic information

in order to comply with Federal, State, tribal, or territorial reporting, evaluation, or data collection requirements

d. IMF recognizes that it does not possess any ownership interest in the samples and resulting data entrusted to it. Consequently, IMF shall not compile, sell, license, transfer, share, or otherwise make available to third parties any data, including deidentified data, generated or derived from the samples from a victim, crime scene, suspect.

6. Information from external sources
    a. Confidential information obtained from sources other than the client also remain confidential in the same manner as the above listed client confidentiality policy. Additionally, the source of the information about the customer is kept confidential from the customer, unless agreed upon by the source his/her/their identity to the customer.
7. Customer Notification of Lawfully Required Disclosure/Subpoenas
    a. Unless specifically disallowed, any lawfully required release of confidential information will elicit notification of the affected party (client etc.) of the release of information.
    b. In an effort to protect the privacy and safety of the persons affected by the release of information, any release requests that include personally identifiable information as defined by the Definitions of Title 34 – Crime Control and Law enforcement of the United State Code, shall be reviewed by the CEO, presently a licensed attorney, prior to release.
8. Breaches of Personally Identifiable Information
    a. In the event a breach of personally identifiable information occurs or is determined to be imminent, all applicable grantors shall be notified of the breach within 24 hours of the detection of the actual breach or imminent breach occurs.
        i. Applicable grantors include any Federal, State, tribal, or territorial organizations.
    b. Once a breach or an imminent breach has been identified, immediate efforts will be made to identify the source and extent of the breach.
        i. Once the source has been identified, efforts will be made immediately to rectify the issue that caused/allowed the breach, to prevent future occurrences from happening in the same manner.
            1. Documentation of the notification will be maintained in writing.
        ii. Once the extent of the breach has been identified, notification to all impacted parties as well as all applicable grantors will be made to provide further information in support of the initial notification.
            1. Documentation of the notification will be maintained in writing.
9. Vendor/Contractors
    a. Any Vendors and/or Contractors doing work for and with Intermountain Forensics are required to maintain the above level of confidentiality.
    b. If any confidential information will be accessible, an NDA/Confidentiality agreement will be signed prior to the access being allowed.
        i. If Confidentiality is included in the contract agreement, it made be used in lieu of a separate NDA/confidentiality agreement.

4. References

N/A

5. Definitions

Personally identifying information (34 USC § 12291(a)(25)): individually identifying information for or about an individual including information likely to disclose the location of a victim of domestic violence, dating violence, sexual assault, or stalking, regardless of whether the information is encoded, encrypted, hashed, or otherwise protected, including— (A) a first and last name; (B) a home or other physical address; (C) contact information (including a postal, e-mail or Internet protocol address, or telephone or facsimile number); (D) a social security number, driver license number, passport number, or student identification number; and (E) any other information, including date of birth, racial or ethnic background, or religious affiliation, that would serve to identify any individual.