

MEDX12, Inc.
9750 Ormsby Station Road
Louisville, Kentucky 40223

NOTICE
OF
MEDX12 PRIVACY AND SECURITY
POLICIES & PROCEDURES
(INCLUDING HIPAA COMPLIANCE)

[Overview; Posted on MedX12 Website]
(Revised, February 2009)

THE INFORMATION SET FORTH BELOW AND THAT APPEARING IN THE MEDX12 ONLINE PRIVACY AND SECURITY STATEMENT ON OUR WEBSITE, DESCRIBES HOW INFORMATION THAT YOU SUPPLY TO US, INCLUDING MEDICAL INFORMATION ABOUT YOUR PATIENTS, IS USED AND PROTECTED AND HOW YOU OR THEY CAN GET ACCESS TO ANY SUCH INFORMATION THAT IS STORED BY US. TOGETHER, THESE STATEMENTS PROVIDE YOU WITH REQUIRED NOTICE OF PRIVACY, SECURITY, AND CONFIDENTIALITY POLICIES AND PRACTICES OF MEDX12, IN CONFORMITY WITH HIPAA AND FEDERAL AND STATE CONFIDENTIALITY STATUTES.

I. ABOUT THIS PRIVACY AND SECURITY POLICY GUIDE.

We at MedX12, Inc. (we refer to ourselves as “we”, “MedX12” or as the “Company” in this document) understand how important privacy and security is to our customers, relating both to their own personal information and to any individually identifiable healthcare information of their patients that they relay to us for claim transaction processing and submission to payers and for the other products or services offered through MedX12 for which you contract. MedX12 is committed to honoring your privacy and security rights regarding this information and that of your patients, and to offering special protections for any individually identifiable healthcare information transferred to us. This document contains an overview of important privacy and security policies and procedures adopted by MedX12 for both the public (opened to members and visitors alike), and private (open to our customers, after required authentication) portions of our Web site.

This privacy and security policy guide applies to certain private patient and provider (customer) information (medical—under HIPAA, and other—for example, financial) that we receive through our Web site (www.MedX12.com) and its use by healthcare providers and payers, and their representatives, to whom it is transferred pursuant to agreements we enter with our customers and business associates. The policies and procedures cover our efforts to assure privacy and security of certain information provided through use of our products, for example, the information transferred as part of the use of our healthcare claim submission and processing services and products, services, and reports related to these products. These policies and procedures are also intended to be utilized in regard to other confidential information received by us from our customers or other parties in contract with us that is not covered by HIPAA, with our implementation being governed by the applicable Federal and state information protection statutes governing confidential use and storage of each different information category.

The “Health Insurance Portability and Accountability Act of 1996, as amended”, and the regulations promulgated under it (referred to in this document as “HIPAA”) contains the major Federal statutory mandates regarding the privacy and security of protected healthcare information (as defined in HIPAA) as it is used and transferred by entities in the healthcare industry. For your information, we have set forth below an overview of the major HIPAA privacy and security policies implemented by MedX12, in regard to our protection of individual patients’ healthcare information provided to us via our Web site.

Please be aware of the fact that, since the privacy and security policies described below only apply to MedX12’s Web site and activities related to it, you should read the policies posted at each Web site that you visit after you leave our site, especially if you are referred or linked to it (them) from our site. We are not responsible for how other Web sites treat your privacy, once you leave our Web site. We enter HIPAA business associate agreements with all third parties with which we contract for provision of products or services to us, some of which are offered to our customers. These agreements contain extensive provisions regarding HIPAA privacy and security protections that the parties undertake to observe.

II. INFORMATION WE COLLECT.

A. Information We Collect From Non-Subscriber Visitors.

Visitors to our Web site can access the Web site’s home page, and browse some areas of the site, without disclosing any individually identifiable healthcare information. We do track information provided to us by your browser, including the Web site you came from (known as the “referring URL”), the type of browser you use, the time and date of access, and other information that does not personally identify you. A person/entity must enroll with us to use much of the site. Little of the information requested of non-subscriber visitors is in any way affected by HIPAA mandates. (See the MedX12 “Online Privacy and Security Statement.”)

B. Information We Collect When a Customer Registers/Enrolls; Information We May Transmit.

1. A customer registering or enrolling for use of our claims processing services, whether the registration is done on our Web site or via a paper contract entered into by MedX12 and the customer, is asked to provide us with identifying information, such as name, address, and contact information. (By “customer” we mean a provider of healthcare services or goods for which reimbursement or compensation may be sought from a third party payer through use of our Web site and associated software.) On our registration screen and in our contracts we clearly specify what information is required for enrollment, and what information is optional and may be given at your discretion. Our Web site’s sign-up form requires users to give us contact information (i.e., name, address, phone number, e-mail address), unique identifiers (i.e., Tax ID#, EIN# or SSN#), and certain financial information (for billing purposes). The user’s contact information is used by MedX12 to contact the user when necessary. Users may opt-out of receiving certain mailings by contacting their designated Customer Service representative. **MedX12 allows users to correct and update their personal information at any time by changing their Personal Profile on-line.**

2. After enrollment, customers will utilize our Web site to securely transmit certain protected health information of their patients to insurance payers, special clearinghouses, or other healthcare service providers whose products/services our customers have requested.

C. Certain Required Release of Information.

We may be required to release account and other personal information of customers and their patients when we believe release is required to comply with law. We will

only release individually identifiable health information, including information from a medical record, if, in our best judgment, after review by our attorney, the release is compelled by law or regulation, or if the release is necessary to prevent the death or serious injury of an individual. It is the Policy of MedX12 not disclose individually identifiable healthcare information from patients' medical records (or, indeed, any other individually identifiable information) to an unrelated third party unless that disclosure is authorized in writing by the owner of the information (patient or customer), the caregiver or healthcare provider for medical purposes, as appropriate, whether for treatment of the patient, or payment of claims, or otherwise.

When we share information with third parties under terms of our product agreements, we ask that they agree in writing to abide by MedX12's privacy/security policies. If we discover that a third party inadvertently disclosed personal information about any of our customers or their patients, we will take immediate action to prevent further occurrences.

III. MEDX12 HIPAA-RELATED PRIVACY POLICIES/PROCEDURES.

As of the date of this overview of MedX12's HIPAA Privacy and Security Policies and Procedures, the Company complies with all regulations on transaction sets and privacy and security requirements and suggested procedures covering protected health information, as defined, including implementation of business associate and chain of trust protocols with all entities involved in our clearinghouse and other intermediary services to our customers.

A. Important Definitions Governing HIPAA Privacy and Security.

1. "Covered Entity" is defined in HIPAA, 45 C.F.R. Section 160.103 as:

- (a) A health plan.
- (b) A health care clearinghouse.
- (c) A health care provider who transmits any health information in electronic form in connection with a transaction covered under Part 160.

2. "Business Associate" is defined in HIPAA, Section 160.103 as:

- (a) A person (entity) that, on behalf of a "Covered Entity" or an "Organized Health Care Arrangement" (164.501) in which the Covered Entity participates, performs or assists in performance of a function or activity involving the use or disclosure of individually identifiable health information (including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and re-pricing); or which provides, other than in the capacity of a member of the workforce of such Covered Entity, legal, actuarial, accounting, consulting, data aggregation (as defined in Section 164.501), management, administrative, accreditation, or financial services to or for such Covered Entity, or to or for an Organized Health Care Arrangement in which the Covered Entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such Covered Entity or arrangement, or from another Business Associate of such Covered Entity or arrangement to the person.

- (b) A Covered Entity may be a Business Associate of another Covered Entity.

3. "Healthcare Provider" means a provider of services (as defined in Section 1861(u) of Social Security Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Social Security Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

4. "Healthcare Plan" includes, singly or in combination:

- (a) a group health plan;
- (b) a health insurance issuer;
- (c) an HMO;
- (d) Part A or Part B of the Medicare Program under title XVIII of the Social Security Act;

- (e) miscellaneous others.

5. “Healthcare Clearinghouse” is defined in HIPAA as a public or private entity, including billing service, re-pricing company, community health management information system or community health information system, and “value-added” networks and switches, that either:

- (a) processes or facilitates processing of health information received from another entity in a non-standard format or containing nonstandard data content into standard data elements or a standard transaction;

- (b) receives standard transactions from another entity and processes or facilitates processing of health information into non-standard format or nonstandard data content for the receiving entity.

6. “Individually Identifiable Health Information” is defined in HIPAA Part 164—Subpart E (Privacy); Section 164.501 (Final Rule) as: “Information that:

- (a) Is created or received by a health care provider, health plan, employer, 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) Which identifies the individual, or

- (ii) With respect to which there is a reasonable basis to believe that the information can be used to identify the individual.”

7. “Protected Health Information” or “PHI” is defined in HIPAA, at 45 C.F.R. 164.501 (Part 164---Subpart E (Privacy); Section 164.501 (Final Rule)), as “Individually Identifiable Health Information” that is:

- (a) Transmitted by electronic media;

- (b) Maintained in any medium described in the definition of electronic media at Section 162.103 of this subchapter; or

- (c) Transmitted or maintained in any other form or medium.

8. “Electronic Media” is defined in Section 162.103 as: The mode of electronic transmission, including the Internet (wide open), Extranet (using Internet technology to link a business with information only accessible to collaborating parties), leased lines, dial-up lines, private networks, and those transmissions that are physically moved from one location to another using magnetic tape, disk, or compact disk media. Further, “electronically transmitted” includes information exchanged with a computer using electronic media, such as the movement of information by magnetic or optical media, transmissions over the Internet, Extranet, leased lines, dial-up lines, private networks, telephone voice response, and “faxback” systems. “Electronically maintained” means information stored by a computer or on an electronic medium from which information may be retrieved by a computer, like electronic memory chips, magnetic tape, magnetic disks, or compact disc optical media.

B. HIPAA Privacy and Security Team and Contact Person; Policy Changes.

1. MedX12 has designated a HIPAA Privacy (and Security) Team (“Team”) that reports to senior management on implementation of policies and procedures adopted by the Company in compliance with its HIPAA responsibilities. The Team makes regular reports to management regarding HIPAA compliance and matters that may have

arisen requiring correction or amendment to such policies. The Team will also inform management, and prepare information for dissemination to employees, of new mandates under the Privacy and Security regulations. The Team includes representatives of Company departments with responsibility for information technology, product development and management, legal/financial, and executive management functions. The Team and a designated Contact person will be accountable for MedX12's policies and procedures and compliance with the HIPAA statutes, as they evolve.

2. MedX12 annually reviews the status of HIPAA privacy and security protections and Team performance, and authorizes any reasonable amendments to policies and procedures. If the Company determines that our HIPAA privacy and security policies must be amended in significant ways, we will make every effort to notify you of the changes. For minor changes to the policy that will not affect our use of your individual information or your patients' individually identifiable health information, we will note the change at the end of the policy statement. When the policies change in a way that significantly affects the way we handle PHI, we will not use the information we have previously gathered or accumulated without obtaining consent from the appropriate individual/entity. We will post major privacy/security policy changes on our Web site in a timely manner.

C. Complaint Process.

1. MedX12 has designated members of its Privacy Team as the contacts responsible for receiving any complaints or action requests regarding MedX12's privacy practices and use or access to protected information. Each complaint/request will be documented, as will the disposition of each, by the Team. The records shall be retained for 7 years.

2. The Company takes all appropriate steps to assure that neither MedX12 nor any of its employees, business associates, vendors, or known agents shall threaten, intimidate or retaliate against any individual or entity who/which files a complaint.

3. The Company is prepared to respond to HIPAA-based complaints or related requests for access to information in one of the following ways:

(a) Denial of Access. MedX12 personnel familiar with information regarding a received complaint may determine, on behalf of the Company, and with due documentation, to deny a complainant access to his/her PHI. MedX12, in compliance with HIPAA, will respond to a complainant with an explanation of its denial rationale and will give the complainant information on how it may complain to the Secretary of HHS—giving the name of the Privacy Team member making said determination, or simply referring to the determination as that of the entire Team and setting forth the Team's telephone number for further communication.

(b) Denial of Amendment. If MedX12 (through its Privacy Team) denies a request to amend a medical record that may be in the possession of MedX12 (a rare situation that must be authenticated with management and with MedX12 customer prior to any response to a requestor), the Company will explain its denial of amendment to the requestor, and indicate how it may complain to the Secretary of HHS as well.

(c) Facilitation of Investigations Arising from a Complaint or Request. If, as a result of a complaint or request to the Secretary of HHS, MedX12 is investigated for its response by HHS, the Company will permit access to information about the matter of the complaint/request during normal business hours (or at any time and without notice, if the Secretary determines that the circumstances warrant—and provides immediately a justification therefore).

D. Documentation of HIPAA Policies and Procedures.

1. MedX12 maintains all HIPAA related policies and procedures, and amendments thereto, in writing. Access to such policies and procedures is assured to our

customers and their patients, as applicable, upon receipt of appropriately authorized requests, and also in cases of a Secretary of Health and Human Services review or request.

2. Documentation materials shall be stored for no less than 7 years, and appropriate means of destruction or return shall be developed and maintained.

3. Company procedure provides for documenting any and all designated record sets in its possession that are readily accessible by individual owners (including the titles of employees responsible for receipt and processing of requests for access). MedX12 guarantees an individual's right of access to inspect and obtain a copy of any of the individual's PHI in current use or possession of the Company or in storage controlled by the Company for as long as such PHI is kept in a designated record set (readily identifiable to the individual).

4. MedX12 guarantees individuals the right to receive an accounting of any disclosures of their PHI of which it becomes aware upon request (if in relation to a Business Associate agreement, where the other party controls the PHI, MedX12 must seek the approval of the referring Business Associate prior to any access arrangements). In order for MedX12 to provide this information, and only to the extent information is available or MedX12's functions were materially affected, MedX12 will document and retain:

- The dates of PHI disclosure;
- The names of entities receiving the PHI, and address, if known;
- A brief description of the disclosed PHI;
- A brief statement of the purpose of the disclosure (if in Business Associate role, reference to the contract is appropriate);
- A copy of any written accounting supplied to the individual (unless answered in Business Associate role, in which case the identity of the prime Associate which provided the accounting should be stored); and,
- Titles of employees responsible for receiving and processing the accounting.
- Signed Authorizations;
- Complaints on HIPAA matters received, and their disposition;

E. MedX12 Employee Policies: Sanctions for HIPAA Violations; Training.

1. MedX12 has instituted a sanctions regime in regard to workers and agents that imposes warnings and sanctions appropriate to the nature of the violation of HIPAA or the Company's policies and procedures. Different levels of sanctions will be determined by factors such as severity of the violation, intentional or unintentional nature of the violation, patterns of improper use and disclosure or single events, etc., and shall range from warnings to termination.

2. MedX12 has all employees and selected agents sign new Confidentiality and Non-Disclosure Agreements that include description of HIPAA regulations and possible sanctions to be imposed for violation. Any employment contracts issued by MedX12 contain a separate provision regarding the Company's sanctions policies in regard to misuse or inappropriate disclosure of PHI.

3. MedX12 has developed methods and materials with which to train its workforce on an annual basis of HIPAA responsibilities and the Company's policies and procedures addressing them. Although a formal register of employee attendance is not required, the Company collects signatures of workforce members attending initial HIPAA training, and stores the document in employee files, showing compliance with the training standard. The Company will develop review tests for yearly training sessions.

F. Requests for an Accounting of Disclosures of PHI to Customer's Patients*

** Note: It is important whether MedX12 is operating as a Covered Entity or a Business Associate regarding the affected PHI, since if it is a BA, the BA Agreement, ONLY, Controls a BA's Response and Patient Rights against BA.*

1. MedX12 guarantees individuals the right to receive an accounting of disclosures of PHI (whether MedX12 is in contact with such through a Covered Entity [direct service] or Business Associate [only after approval by its referring Business Associate] capacity) during the established retention period, in conformity with agreements with customers and business associates bearing upon the subject PHI. Actual disclosures depend upon facts of each disclosure circumstance and the contracts with customers or business associates related to them. Tracking procedures include designation of the recipient of the request (with the Team as its designated agent), establishing the response time, setting the final form of the disclosure accounting, and determining the means of delivery (and collection of fee, if appropriate).

2. MedX12 has developed a form by which individuals may request such an accounting (in most cases MedX12 is aware that it will receive accounting requests from a Covered Entity to which it provides services as a Business Associate).

G. Access, Inspection, and Copying of PHI. *

** See Note to III.F., above.*

1. MedX12 guarantees an individual's right of access to inspect and obtain a copy of any of the individual's PHI in current use or possession of the Company or in storage controlled by the Company for as long as such PHI is kept in a designated record set (readily identifiable to the individual).

2. MedX12, whether acting in a given situation as a Business Associate, subject to another Business Associate or Covered Entity through contract, or as a Covered Entity under these policies, will document and retain the following information for 7 years regarding access and copying of PHI by the individual owning such information, after due authentication:

- Designated Record Sets subject to access;
- Titles of persons/offices responsible for receiving and processing access;
- Written requests for access;
- Written denials; and,
- Written statements by the Covered Entity establishing extension of response time.

3. MedX12 will provide any individual requesting PHI access with a simple request form to complete. After receipt of a request, the Company will follow appropriate procedures for processing requests for PHI and access to it, overseen by the Privacy Team.

H. Requests for Amendment to, or Restrictions on, Uses/Disclosures of PHI.

1. MedX12 guarantees an individual whose PHI is currently being used by it, or is in storage (under its control), the right to request amendment of said PHI or a record about the individual, for as long as the information is maintained in a designated record set (documents maintained in single "file," providing ready identification of the individual). Company decisions on appropriateness of any amendment request shall be documented and stored with the PHI for required storage period.

2. The Company policies regarding requests by individuals for restrictions on use and/or disclosure of their PHI require review of each case separately, including Company contracts with customers and business associates that affect the individual's request.

(a) Upon receipt of an appropriately filed request for restrictions on use/disclosure of PHI from an individual/owner, the MedX12 Team representative will discuss the restrictions request with the individual, to assure that they are in the individual's best interest. This will rarely affect MedX12 in its Business Associate role.

(b) The MedX12 Privacy Team, in consultation with the Covered Entity involved, will establish how any restriction agreed upon with the individual will be documented and implemented so as not to cause harm to the individual in future, unforeseen circumstances.

I. Required Authorizations Affecting Use and Disclosure.

1. MedX12's products and services on the date of this Policy do not require our solicitation of individual authorizations for access to PHI (other than, possibly, in marketing situations). The Company may be required to store any authorizations that it receives from its customers/business associates for continued reference, or for historical documentation purposes and the MedX12 policy requires a business associate or similar agreement with a customer to cover all authorizations to which such entity, and or patients covered by such, are to have access.

2. MedX12 has developed a form authorization, compliant with all HIPAA requirements, that may be utilized in cases where it is required that we (or a customer or business associate) seek an individual's (patient's) authorization to use his PHI.

J. Policy on De-Identification of PHI.

If MedX12 is called upon, as a Business Associate of a Covered Entity, to "De-Identify" any PHI for its eventual use for permissible activities (usually in aggregated surveys), it will remove individual identification on any PHI concerning the individual owner (patient) of the PHI and also similar information on his relatives, employers, or household members as may exist in our records. Included in information subject to any de-identification procedure are: Names; All geographic subdivisions smaller than a state (including street address, city, county, precinct, zip code, and their equivalent geo-codes, except the initial three digits of the zip code); All elements of dates (except year) for dates directly related to the individual (including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of age, except that such ages and elements may be aggregated into a single category of age 90 or older); Telephone, FAX numbers; E-Mail addresses; SSNs; Medical record numbers; Health plan beneficiary numbers; and, any other unique identifying number, characteristic or code.

K. Verification of the Identity and Authority of Entities Requesting PHI.

1. MedX12 must verify the identity and authority of any person requesting use or disclosure of PHI in MedX12's possession. The verification requirements include documenting knowledge of the person's place of business, address, phone number or fax number, and authentication of his citizenship via SSN or otherwise. Additional authentication may be required when the law requires additional proof (in crime or abuse situations, especially).

2. The Company has also developed requirements for verifying the identity and authority of public officials requesting PHI in the Company's possession.

3. In some instances, the Company may require a power of attorney from a person claiming to be a representative of the individual owning the PHI, or, in the case of family members, proof of family status.

IV. MEDX12 HIPAA-RELATED SECURITY POLICIES AND PROCEDURES.

A. General Policies.

We have implemented technology and security policies, rules, procedures, and other measures to protect the personally identifiable data of customers and their patients that we

have under our control from unauthorized access, improper use, alteration, unlawful or accidental destruction, and accidental loss. We also protect this information by requiring that all of our employees and others who have access to or are associated with the processing of this data respect your confidentiality, and confirm this obligation to you by signing a confidentiality agreement with us.

Where we allow a healthcare provider or payer to access actual medical records created by a healthcare provider, we require that the browser used support a high level of encryption to reduce security risks.

MedX12 uses secure methods to determine the identity of its registered users, so that appropriate rights and restrictions can be enforced for the user. Reliable verification of user identity is called authentication. MedX12 uses both passwords and usernames to authenticate users. Users are responsible for maintaining their own passwords.

NEVER SHARE YOUR MEDX12 USERNAME OR PASSWORD WITH ANYONE WHO IS NOT AUTHORIZED TO ACCESS YOUR ACCOUNT.

PLEASE USE THE “LOG OFF” BUTTON WHEN EXITING THE MEDX12 WEB SITE; THIS ENDS YOUR SESSION AND HELPS PREVENT UNAUTHORIZED USERS FROM ACCESSING YOUR ACCOUNT.

B. Security Practices and Technology.

1. Positive User Identification – Access to our system, past the entry-level Web site information pages, is restricted to authorized users only. Users must supply a user ID and a password to access their information on our Web site. Users who forget their password must pass our challenge/response process to ensure legitimacy before being given their forgotten password.

2. Positive Site Identification – The MedX12 Website is registered with the Verisign™ site certification authority to enable a user’s Web browser to confirm the site identity before proceeding. With this technology, the identity of MedX12’s site is confirmed to the browser. If positive identification is not made, the user’s Web browser notifies the user that the receiving site is suspicious.

3. In-Transit Data Encryption – All data being passed between the user’s browser and the private portion of MedX12’s Website is encrypted. This information is transmitted using Secure Sockets Layer (SSL) technology with 128-bit encryption.

4. Information Back-up – All sensitive information in our office data center is backed up routinely, in order to aid in the recovery of information in the event of accidental damage of information or due to a natural disaster. The backup media is stored in a physically secure storage facility.

5. Application Access Logs – All access to the MedX12 applications is logged to the user level. We thus have a complete record of all users who access our system with dates and times of access.

C. Storage and Protection of Healthcare Information.

Individually identifiable healthcare information of healthcare patients that our customers transmit to us for processing and submitting to payers, back-up information from the office data center, and any sensitive information that we obtain through our relationship with other healthcare professionals, is stored and protected as follows. Note that our third party storage provider is required, by contract, to observe MedX12’s Privacy and Security Policy and keep all information entrusted to it as secure as is technologically possible in conformity with the tenets of commercial reasonability.

1. Firewall Protection – As a front-line defense to the MedX12 system, we have implemented a firewall in front of all public servers. This firewall will help prevent any unauthorized access and guard against Internet hacking attempts.
2. Physical Data Center Security – Our servers are located in a secure hosting facility. This facility requires key card authorization to gain initial entry into the data center. A biometric hand scanner and camera surveillance are available to additionally protect access to the actual server room. The center is monitored 24 X 7 X 365 by the Network Operation Center personnel. MedX12 and the secure hosting facility have coordinated on creation of an emergency recovery plan regarding PHI protection and recovery of utilization.
3. Enforcement of Privacy and Property Protection – MedX12 works with regulators and security professionals, including our own security firm, local police, the Federal Bureau of Investigation, and the Internet security division of the U.S. Postal Service to assure against, or speedily locate and abort, Internet-based or other attempts to access personally identifiable healthcare (or financial) data that we have in our possession or transmit for customers. Our Customer Service personnel keep in contact with customers regularly to determine any payment or transmission problems that may indicate illegal access attempts by third parties that would trigger our immediate response.

V. PRIVACY AND SECURITY QUESTIONS.

For privacy questions or concerns about MedX12's Website and Company policies reviewed on it, please contact us at one of the following:

E-Mail --- support@MedX12.com;

Visit --- www.medx12.com;

Call --- (502) 339-7175