Protection of Privacy for Benemax Clients

How Benemax safeguards our clients' private information...

A. Legal Regulation

Benemax takes pride in the care with which we protect the privacy of our clients and of their employees. Their trust in our professionalism is essential to our success. We also recognize our obligations under the various laws which exist to guarantee that privacy. Below is a summary of these laws and their major provisions.

1. HIPAA - Privacy Rule

The HIPAA Privacy Rule, which took effect in April of 2003, regulates the use and disclosure of certain information held by "covered entities" (generally, health care clearinghouses, employer sponsored health plans, health insurers, and medical service providers that engage in certain transactions. It establishes regulations for the use and disclosure of Protected Health Information (PHI). PHI is any information held by a covered entity which concerns health status, provision of health care, or payment for health care that can be linked to an individual. This is interpreted rather broadly and includes any part of an individual's medical record or payment history.

As a Business Associate, Benemax is bound by the Privacy Rule. We are required to take measures to ensure that PHI is not disclosed except to the individual member or to covered entities engaged in providing claims service. These measures are discussed in more detail below.

In addition to the Privacy Rule, HIPAA also requires that we maintain reviewable records of our PHI related transactions for up to seven years; that we make PHI available to individual members upon request; that we correct any PHI details which are in error; and that we establish and maintain an internal advocacy to protect our clients rights under HIPAA.

Benemax is in full compliance with these regulations. We have been successfully audited regarding this compliance and we are committed to maintaining our track record.

2. Protection of Personal Information of Residents of the Commonwealth of Massachusetts – M.G.L. c.93H, 201 CMR 17.00

The Massachusetts Regulation is intended to protect individuals from fraud and/or identity theft by requiring all persons who obtain personal information to protect this information by...

- Ensuring the security and confidentiality of the information in a manner consistent with industry standards;
- Protecting against anticipated threats to the security of such information;
- Protecting against unauthorized access to or use of such information.

The law defines personal information as a person's name, social security number, driver's license or state issued ID number, and financial identification including account number, credit card number or debit card number. The law excludes any information which can be obtained from publicly available sources.

Again, Benemax is bound by this law and Regulation to comply with its requirements for protecting personal information which we obtain from our members in the course of serving their service needs.

We understand that, from time to time, other requirements may be placed on Benemax by regulating agencies. We have a highly qualified, full time compliance officer on our staff, who reviews emerging regulatory requirements and informs Benemax management and employees about their obligations under these rules.

B. Benemax Operations

Privacy Officers – The regulations require that Benemax appoint privacy officers who assume operational responsibility for ensuring ongoing compliance. These officers are:

1. HIPAA Privacy Officer (HPO) – The HPO has overall authority to define Benemax compliance policies and to enforce their provisions. Contact: David Cowles, David@benemax.com, (508) 242-6117.

2. Compliance Officer (CO) – The CO monitors regulatory developments, reports all changes to Benemax management, and advises how to conform to pertinent regulations. Contact: Kelly Drake, KDrake@benemax.com, (508) 242-6120.

3. Data & Systems Administrator (DSA) – The DSA is responsible for maintaining a technically secure environment as well as for administering and monitoring access to private information. Contact: Dave Earley, DSA, DTE@benemax.com, (508) 242-6102.

4. Information Security Officer (ISO) – Our ISO keeps this Written Information Security Plan (WISP) updated, trains staff in compliance, and audits staff compliance periodically. Our ISO trains every new member of our staff in his or her role in carrying out the Written Information Security Policy (WISP). This training is refreshed annually. If our ISO determines that PHI has been accessed without authorization, he/she will notify the Office of Consumer Affairs & Business Regulation (OCABR) and the Attorney General's Office, describing the theft in detail, and work with authorities to investigate the crime and to protect the victim's identity and credit. To the extent possible, our ISO will also warn the victims of the theft so that they can protect their credit and identity. Contact: Kelly Drake, KDrake@benemax.com, (508) 242-6120.

In addition to making and monitoring policy, Benemax Privacy Officers also conduct (at least) annual reviews of all regulations, policies, and procedures to ensure that our commitment to the members' right to privacy is fully maintained.

Line Management – Day to day responsibility for ensuring that the privacy of our members is guarded carefully is assigned to various line managers, especially with respect to those functions which require us to obtain process and record PHI. These supervisors include, among others, the Claims and Customer Service Manager and the Controller.

If a violation is discovered, the responsible supervisor is required to report the nature of the violation to the Privacy Officers. The violation is documented and appropriate disciplinary action is taken as required. In some cases, if the violation leads to disclosure of protected information to unauthorized parties, the individual member is notified.

Because Benemax manages member information necessary to entering and processing claims, we do obtain private/personal information as a matter of course. Most of this information can be grouped into three broad categories...

Enrollment/Termination information...

When Benemax implements a new client, we solicit enrollment information for their employees so that we can enroll them in the plan which we have constructed for the client. This enrollment information typically includes name, address, gender, date of birth, social security number, etc. Whenever a client adds a covered employee or whenever an employee's status changes, we obtain whatever information is needed to keep our records current. When a client terminates a covered employee, information regarding the date of termination, COBRA election, etc., is also obtained and processed. Benemax treats all information of this type as confidential, consistent with the requirements of the above regulations.

Claims information...

We regularly receive claims information from our insurance provider partners, service providers and claimants. All claims information is assumed to be confidential, and we further assume that it is covered by HIPAA. This means that, in addition to treating claims information as confidential, we also must organize and store it in a secure, accessible manner.

Debit Card information...

Benemax sometimes arranges for members to receive client funded debit cards to pay for specific covered expenses, such as prescription medications, etc. Massachusetts law now requires that we use special care in the storage, retrieval and distribution of debit card account information. In addition, specific transactions using these debit cards may be covered by HIPAA and Federal Trade Commission regulations.

Benemax employees are trained in the specific confidentiality requirements of our business and they are bound by the confidentiality provisions of their employee agreements upon hire and regularly afterwards. Benemax management is charged with monitoring their compliance. From time to time,

Benemax is asked to submit to a review or audit of our procedures and succeed in establishing our compliance with the relevant regulations.

Hard copy information is evaluated upon receipt and either distributed to the intended recipient or stored in a secure storage facility pending processing and disposition. All employees are to keep these documents under cover, except when they are actually processing them. For example, they are never to leave unattended confidential information at a scanner, printer or copier. Outside of normal business hours, the entire facility is secured under lock and key. When these documents have been processed, they are filed in secure filing cabinets and kept on site for a prescribed period of time. Once that time has elapsed, they are archived. Archived hard copy documents are kept in an offsite storage facility, also under lock and key and further secured by camera surveillance. Our employees are also not to remove any covered documents from the premises. Remote workers are subject to all of the same requirements and safeguards with respect to covered information. All covered documents which Benemax is not required to store are shredded and disposed of in a secure manner.

Facsimile (fax) – Benemax uses electronic faxing, both inbound and outbound. Inbound faxes can be sent directly to the appropriate Benemax associate's desktop, to a general purpose claims input area or to a general fax number. In all cases, these faxes are routed through our secure business server, either directly to the intended recipient or to an electronic folder. Faxes which are placed in a general folder are individually reviewed and distributed, still in electronic form and using our secure e-mail server. Outbound faxes, consisting of scanned original documents, or of electronic files, are sent directly from the individual sender's desktop to the recipient's fax facility through the fax server function on our secure business server. We do not use a paper fax machine, except as a backup to our main server. Because faxes at Benemax are electronic, they are inherently more secure than their paper equivalent and the distribution, use and storage of faxes is more efficient.

Electronic Records – Our e-mail facility is a secure Microsoft Exchange Server, which is located in our headquarters server farm. The server farm is located in a double locked room and access to it is limited. The Exchange Server is behind a tightly configured firewall. Access to the server is very closely controlled. E-mail accounts are limited to employees and their access to e-mail is only through User-ID and password, assigned and controlled by the system administrator. Both inbound and outbound e- mails pass through two layers of active scanning for detection of unwanted attachments and content. Remote access to Benemax e-mail is permitted, but is also secured by User-ID and password. As with hard copy, externally accessed e-mails are typically limited to information which is not considered confidential. E-mail traffic is constantly monitored, using both automated tools and regular review by management.

Benemax maintains a client services website – http://www.virtualbenefitmanager.com – at which members can submit claims, check on the status of prior claims and perform other related functions. Some of these transactions are subject to the same privacy regulations as are offline transactions. In each and every case, the forms which are used for these transactions are encrypted and the site is secured by a trusted certificate. The forms are then delivered via secure e-mail to the appropriate group for processing.

Apart from e-mail, other forms of electronic records are also secured. Large file transfers (such as monthly claims reports) are retrieved using ad-hoc encryption from a secure FTP site. E-mail security guards small file transfers in the form of e-mail attachments.

We also, as a matter of course, turn many hard copy records into electronic objects by scanning them, in order to improve efficiency. Scanned documents are either shredded or filed in a secure facility. Scanned objects are placed in internally available object repositories. These repositories are only made available to employees who are logged on to the domain inside the firewall. All electronic records are backed up daily onsite. When electronic objects reach a certain age, they are archived. These archives are also kept on the secure domain, behind the firewall.

When a Benemax employee is terminated for any reason, their access to secure domain assets is turned off immediately.

C. Vendor Compliance

We routinely share PHI in the form of employment records, pension and insurance information, and other information required to be a responsible employer. We share this PHI with the state and federal tax authorities, our payroll service, our 401(k) provider and our CPA firm. Our IT Service Provider sometimes may see PHI in the course of repair work and consulting. We require each of these organizations to send us a letter, signed by their CEO or other authorized person, that they follow a Written Information Security Plan (WISP) that fully complies with 201 CMR 17.00. The only exception is the state and federal tax authorities, which we assume are compliant, since they must comply with laws that are stricter than 201 CMR 17.00.

Visitors to Benemax are not admitted to work space where protected information is accessible.

D. PHI on Computer Systems

All PCs, laptops and workstations of individuals will be secured with a password-protected screensaver with the automatic activation feature set at 20 minutes or less. When they walk away from their desk they will use the Windows-L key combination to lock their screen.

All PHI stored on the Benemax network is protected using our Corporate Password Policy (see Appendix A).

PHI stored on laptops and portable devices must be encrypted using the authorized systems provided for this purpose.
Only Benemax provided portable devices can be used to store Corporate Information.

All emails and documents including PHI must be encrypted using the Benemax Corporate Email Encryption System.

Passwords are not to be transmitted by email. We use Strong Encryption with a password arranged in person or by SMS, fax or telephone.6