Laercio M. da Silva Jr W0433181

Date: Oct 18th

**Health Billing System - Policy and Procedure Management**

**Security Passwords -** In the Health Billing System (HBS) passwords are a critical component of information security. Passwords are for each user to maintain secure access to their HBS accounts, but if the password is weakly constructed it can result in compromised HBS security.

This section aims to recommend practices for creating strong passwords and is aimed at employees, contractors, consultants, temporary workers and other Medavie Blue Cross workers.

For a password to be strong it must be long, that is, the more characters the password has, the stronger it is. The recommendation for HBS is a minimum of 10 characters and a maximum of 14 characters. In addition, the password must have a capital letter, a lower case letter, a number, and a special character (! @ # $% & \*).

The password cannot have an alphabetical (abcde) or numeric (12345) sequence. Nor can they repeat the same character more than 2 times (atttfo).

The password verification will be done automatically by a script when the user tries to create a new password. Users will only be able to create a new password if they meet the requirements stated above.

It is also strongly recommended that HBS users do not share their passwords and consequently their access accounts with other people. A user who has violated this policy may be subject to disciplinary action.

**Security User Access Rights -** This Privacy Policy contains information about how we treat, in whole or in part, in an automated or non-automated way, the personal data of users who access HBS. Its purpose is to inform stakeholders about the types of data that are collected, the reasons for the collection and how the user can update, manage or delete this information.

This Privacy Policy was prepared in accordance with the most current laws to protect the user's privacy. HBS is committed to complying with the rules set out in respect of the following principles:

* The user's personal data will be processed in a lawful, loyal and transparent manner (lawfulness, loyalty and transparency);
* The user's personal data will be collected only for specific, explicit and legitimate purposes, and cannot be further processed in a way incompatible with those purposes (limitation of purposes);
* The user's personal data will be collected in an appropriate, relevant and limited way to the needs of the purpose for which they are processed (data minimization);
* The user's personal data will be accurate and updated whenever necessary, so that the inaccurate data is deleted or rectified when possible (accuracy);
* The user's personal data will be kept in a way that allows the identification of the data holders only for the period necessary for the purposes for which they are processed (limitation of conservation);
* The user's personal data will be treated securely, protected from unauthorized or illicit treatment and against its accidental loss, destruction or damage, adopting the appropriate technical or organizational measures (integrity and confidentiality).

The HBS user has the following rights:

* Right of confirmation and access: it is the user's right to obtain from HBS the confirmation that the personal data concerning him are or are not subject to treatment and, if that is the case, the right to access his personal data;
* Right of rectification: it is the user's right to obtain from HBS the rectification of inaccurate personal data concerning him;
* Right to delete data (right to be forgotten): it is the user's right to have their data deleted from HBS;
* Right to limit the processing of data: it is the user's right to limit the processing of his personal data, obtaining it when he disputes the accuracy of the data, when the processing is illegal, when the website no longer needs the data for the purposes proposals and when opposed to the processing of data and in case of processing unnecessary data;
* Right of opposition: it is the user's right to oppose, at any time, for reasons related to his particular situation, to the processing of personal data concerning him, and may also oppose the use of his personal data for profile definition marketing (profiling);
* Right not to be subjected to automated decisions: it is the user's right not to be subject to any decision taken exclusively on the basis of automated treatment, including profiling, which has an effect on its legal sphere or which significantly affects it similarly.

The user can exercise his rights through written communication sent to the information security team specifying: Full name and e-mail address of the user and, if applicable, of his representative; Right you want to exercise with the website; Order date and user signature; Any document that can demonstrate or justify the exercise of your right. The request should be sent to informationsecurity@hbs.com.

The collection of user data will be in accordance with the provisions of this Privacy Policy and will depend on the user's consent.

The use, by the user, of certain HBS functionalities will depend on registration, in which case, the following user data will be collected and stored: name, e-mail, telephone, job information and professional responsibilities. User access records will also be collected and stored for at least six months.

Eventually, other types of data not expressly provided for in this Privacy Policy may be collected, provided that they are provided with the user's consent, or that the collection is permitted or imposed by law.

By using the services of the website, the user is consenting to this Privacy Policy.

The processing of personal data without the user's consent will only be carried out due to legitimate interest or for the cases provided for by law, that is, among others, the following: For the fulfillment of legal or regulatory obligation by the controller; For the conduct of studies by a research body, guaranteed, whenever possible, the anonymization of personal data; When necessary for the execution of a contract or preliminary procedures related to a contract to which the user belongs, at the request of the data subject; When necessary to serve the legitimate interests of the controller or third party, except where the fundamental rights and freedoms of the data subject that require the protection of personal data prevail.

The personal data of the user collected by the HBS are intended to facilitate, streamline and fulfill the commitments established with the user. The registration data will be used to allow the user to access certain contents of the HBS.

The user's personal data will be kept for a period not exceeding that required to fulfill the purposes for which they are processed.

HBS undertakes to apply technical and organizational measures capable of protecting personal data from unauthorized access and situations of destruction, loss, alteration, communication or dissemination of such data.

To guarantee security, solutions will be adopted that take into account: the appropriate techniques; application costs; the nature, scope, context and purposes of the treatment; and the risks to the user's rights and freedoms.

HBS uses SSL (Secure Socket Layer) certificate which guarantees that personal data is transmitted in a secure and confidential way, so that the data transmission between the server and the user, and in feedback, occurs in a totally encrypted or encrypted way.

However, HBS disclaims liability for the sole fault of the user, as in the case where he himself transfers his data to a third party. The website also undertakes to notify the user in due time if there is any breach of the security of your personal data that could cause you a high risk to your personal rights and freedoms.

The user will be explicitly notified if this policy changes.

**Disaster Recovery -** This policy requires management to financially support and diligently respond to disaster contingency planning efforts. Disasters are not limited to adverse weather conditions. Any event that is likely to cause a prolonged service delay should be considered.

This policy defines a disaster recovery plan to be implemented by Medavie Blue Cross that will describe the process of recovering IT systems, applications and data from any type of disaster that causes a major disruption.

This policy is directed to the IT Management Team, which is responsible for ensuring that the plan is developed, tested and kept up to date.

The following are contingency plans:

• Computer Emergency Response Plan: in case of an emergency, the IT technical support team should be contacted immediately. This team is responsible for carrying out the necessary actions to correct the problem after an analysis of the real situation.

• Succession plan: First, the IT support team must be contacted. If it is not possible to contact this team, you should try to contact the IT manager, and if it is not possible to contact him, you should try to contact the director of the company.

• Data study: all patient and staff data are highly critical and confidential

• Service Criticality List: Database server is highly important. Web Server, Applcation server and Backup server are important. Proxy server is medium importance.

• Data backup and restoration plan: all data contained in the Database Server is also stored on the Backup Server. This data is stored on hard drives and is backed up every 24 hours. In case of loss of data contained in the Database Server, the information security team can be contacted to try to recover the data through the Backup Server.

Management should take the time to test the implementation of the disaster recovery plan. Table exercises must be performed annually. During these tests, problems that can cause the plan to fail can be discovered and corrected in an environment with few consequences.

The plan, at a minimum, must be reviewed and updated annually.

The information security team will verify compliance with this policy using a variety of methods, including, but not limited to, periodic inspection, video monitoring, business tool reports, internal and external audits and feedback to the HBS Administrator. Any exception to the policy must be previously approved by the information security team. An employee who is found to have violated this policy may be subject to disciplinary action, up to and including termination.

**Web Application Security Policy -** It is crucial that any web application is evaluated for vulnerabilities and any vulnerabilities are corrected before the production deployment, however even taking all precautions, some security holes can reach the final version of the system.

The purpose of this policy is to define the security parameters of web applications in the Health Billing System. Assessments are carried out to identify potential weaknesses, weak authentication, insufficient error handling, leakage of confidential information, services available internally and externally, as well as meeting compliance with all relevant policies in force. Thus covering all the security parameters of web applications for the purpose of maintaining the posture of security, compliance, risk management and change control of technologies in use at Medavie Blue Cross.

All web application security assessments will be performed by security personnel delegated, employed or contracted by Medavie Blue Cross. All findings are considered confidential and must be distributed to people based on the “need to know”. The distribution of any discoveries outside of Medavie Blue Cross is strictly prohibited, unless approved by the Chief Information Officer. Subsequent limitations and justifications will be documented before the assessment begins.

Web applications are subject to security assessments based on the following criteria:

* Launch of a new application will be subject to a full assessment prior to the approval of the change control documentation or release in the production environment;
* Web application purchased from third parties will be subject to full assessment, after which it will be subject to policy requirements;
* Point releases will be subject to an appropriate assessment level based on the risk of changes in the application's functionality or architecture;
* Patch releases will be subject to an appropriate assessment level based on the risk of changes to the application's functionality or architecture.
* Emergency releases will be allowed to ignore security assessments and assume the risk assumed until such time as an appropriate assessment can be carried out. Emergency releases will be designated as such by the Chief Information Officer or an appropriate manager to whom this authority has been delegated.

All security issues discovered during assessments must be mitigated based on the following levels of risk. The Risk Levels are based on the OWASP Risk Classification Methodology. The remediation validation test will be required to validate remediation or mitigation strategies for any discovered problems of Medium or higher risk level.

**High** - must be corrected immediately or other mitigation strategies must be put in place to limit exposure before implantation. Applications with high-risk issues are subject to being taken offline or denied release in the active environment.

**Medium** - must be reviewed to determine what is needed to mitigate and scheduled accordingly. Applications with medium risk issues can be taken offline or denied release to the active environment based on the number of problems and if multiple problems increase the risk to an unacceptable level. Problems should be corrected in a patch release, unless other mitigation strategies limit exposure.

**Low** - must be reviewed to determine what is needed to correct the problem and scheduled accordingly.

The information security team will verify compliance with this policy using a variety of methods, including, but not limited to, periodic inspection, video monitoring, business tool reports, internal and external audits and feedback to the HBS Administrator. Any exception to the policy must be previously approved by the information security team. An employee who is found to have violated this policy may be subject to disciplinary action, up to and including termination.

Web application assessments are a requirement of the change tracking process and must adhere to this policy, unless they are exempt. All application versions must go through the change tracking process. Any web application that does not adhere to this policy may be taken offline until such time as a formal assessment can be carried out at the discretion of the Chief Information Officer.

**Remote Access Policy -** Remote access to the corporate network is necessary for some members of the Medavie Blue Cross team. However, this access can originate from compromised networks or a significantly lower level of security than the corporate HBS network. Although these remote networks are outside the control of the corporation, external risks must be avoided to ensure the security of the HBS corporate network.

This chapter aims to define the standards and requirements for remote access to workstations and servers that make up the internal technological environment of HBS, minimizing the potential exposure of the Health Billing System and thus avoiding losses resulting from unauthorized use, and resulting losses exposure of information that compromises public image, social reputation, confidentiality and integrity of HBS's critical systems.

This policy applies to all Medavie Blue Cross employees, namely: employee or commissioned employees, interns, outsourced workers or individuals who directly or indirectly use or support HBS, infrastructure or information. All of these employees will be treated in this policy as users.

Guidelines:

* The remote access of an external network to HBS workstations and servers must be strictly controlled, authorized, using VPN encryption and strong password authentication;
* Requests for remote access to users must be formalized using the specific form, with justification and working period. These requests must be authorized by the area manager or higher and filed for audit purposes;
* The user with authorized remote access will access the same environments that he views internally, that is, he will have the same access profile;
* The authorized users of remote access must protect their credentials and at no time should make their network login and password, e-mail, VPN, or any access information available, to another person;
* Users with authorized remote access must ensure that other people do not use their remote access profile.

Good habits:

* It is recommended that the user with remote access authorization use secure external networks to access the internal environment of the HBS network;
* Users who access the network remotely must be aware that their workstation, notebook, etc., is not also accessing another network at the same time;
* The user, when using remote access, must remain connected only to the HBS network, while effectively using the services provided, and must disconnect during interruptions and at the end of work;
* Users with remote access must ensure that sensitive information is not captured by third parties who are close to the computer.