COMPLEXO DO HOSPITAL DE CLÍNICAS DA UNIVERSIDADE FEDERAL DO PARANÁ
Rua General Carneiro, nº 181 - Bairro Alto da Glória
Curitiba-PR, CEP 80060-900
- http://chc-ufpr.ebserh.gov.br

Norma - SEI nº 13/2024/SUP/CHC-UFPR-EBSERH

Curitiba, *data da assinatura eletrônica*.

USO ADEQUADO DE CREDENCIAIS, COMUNICAÇÃO E ARMAZENAMENTO DE INFORMAÇÕES INSTITUCIONAIS NO ÂMBITO DA SEGURANÇA DA INFORMAÇÃO

O Colegiado Executivo do Complexo do Hospital de Clínicas da Universidade Federal do Paraná, no uso das atribuições legais e estatutárias, de acordo com as competências que lhe foram conferidas pela Portaria nº. 08, de 09/01/2019, publicada em Boletim de Serviço/EBSERH nº 518, p.10, de 09 de janeiro de 2019 (DOU, Edição 7, Seção 1, página 62):

CONSIDERANDO:

- Código de Ética e Conduta da Empresa Brasileira de Serviços Hospitalares (Ebserh) de 2020;
- Lei Geral de Proteção de Dados Pessoais (LGPD);
- Regulamento de Pessoal da Ebserh;
- Política de Proteção de Dados Pessoais da Ebserh;
- Norma Operacional de Uso Seguro de Computação em Nuvem pela Rede Ebserh (SEI nº 6/2022/SGTI/DTI-EBSERH);
- Norma Operacional - SEI nº 1/2021/CCS/PRES-EBSERH;
- Política de Segurança da Informação e Comunicação da Ebserh;
- Política de Segurança da Informação e Comunicação do CHC-UFPR/Ebserh;
- Norma Operacional sobre o Uso Responsável de Unidades Portáteis de Armazenamento de Dados Corporativos e Dispositivos Móveis (SEI nº 5/2020/SGTIC/DTI-EBSERH);
- que este normativo foi elaborado com base nos princípios da segurança da informação e visa promover um ambiente seguro e confiável para o tratamento dos dados institucionais no CHC-UFPR/Ebserh, garantindo segurança jurídica e conformidade com as diretrizes estabelecidas pela Política de Segurança da Informação e Comunicação (POSIC);

DETERMINAM QUE:

Art. 1º Fica instituída esta norma que deve ser aplicada a todos empregados, servidores, terceirizados, docentes, pesquisadores, residentes e alunos que estejam exercendo alguma atividade para este

Complexo do Hospital de Clínicas da UFPR (CHC-UFPR), seja de forma presencial ou remota.

Art. 2º Esta norma tem como objetivo garantir a segurança, confidencialidade, integridade e disponibilidade das informações institucionais, e visa clarificar os deveres e responsabilidades dos usuários em relação ao uso adequado de credenciais, crachás e comunicação, bem como o armazenamento seguro de dados inclusive na nuvem.

Art. 3º São definições:

I. **acesso a dados/sistemas**: consiste no ato de consultar ou processar dados digitais, em caráter temporário ou continuado, por usuários devidamente autorizados;

II. **bloqueio de acesso**: processo que tem por finalidade suspender temporariamente o acesso;

III. **controle de acesso**: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder, bloquear ou revogar acessos ao uso de recursos computacionais;

IV. **contas de acesso**: permissão, concedida por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso aos dados digitais;

V. **revogação de acesso**: processo que tem por finalidade suspender definitivamente o acesso ao dado digital, incluindo o cancelamento do código de identificação e do perfil de acesso;

VI. **usuário**: pessoa física habilitada para acessar os dados digitais;

VII. **dado pessoal**: informação relacionada a pessoa natural identificada ou identificável.

Art. 4º Sobre as **credenciais de acesso**:

I. O acesso aos sistemas e recursos institucionais será concedido mediante o uso de credenciais individuais, compostas por crachá, certificado digital, *login* e senha.

II. É estritamente proibido compartilhar credenciais de acesso com terceiros. Cada usuário é responsável por manter suas credenciais confidenciais e protegidas contra acessos não autorizados.

III. As senhas devem seguir padrões de complexidade definidos pela área de segurança da informação, incluindo comprimento mínimo, uso de caracteres especiais, letras maiúsculas e minúsculas, prazo de expiração e devem ser alteradas regularmente.

IV. Os usuários devem relatar imediatamente qualquer suspeita de comprometimento de suas credenciais de acesso ao Comitê de Segurança da Informação (CSI) por meio do endereço eletrônico: csi.chc-ufpr@ebserh.gov.br.

V. O acesso remoto aos sistemas do CHC-UFPR/Ebserh deverá ser concedido conforme Procedimento Operacional Padrão (POP) estabelecido e divulgado pelo Setor de Tecnologia da Informação e Saúde Digital (SETISD) em: P:\Todos-CHC\POPs e Protocolos Institucionais CHC\Setor Tecnologia da Informação em Saúde (SETISD).

VI. Sempre que possível deve ser usado a Autenticação Multi Fator (*Multi-Factor Authentication – MFA*, em inglês) que é um mecanismo de validação adicional ao processo de entrada (logon ou autenticação) como por exemplo: Tokens, SMS, e-mail, digitais, etc.

VII. É de responsabilidade do usuário manter atualizado o número de telefone celular, e-mail pessoal e/ou aplicativos de autenticação para o correto funcionamento do MFA.

VIII. As permissões de acesso aos sistemas de informação do CHC-UFPR/Ebserh devem ser concedidas pela chefia imediata do usuário. Caso a chefia imediata não tenha privilégios para conceder acessos, o

pedido deve ser encaminhado via GLPI para a SETISD.

IX. Deve ser adotado o princípio do mínimo privilégio, garantindo que os usuários tenham apenas as permissões necessárias para realizar suas funções.

X. Deve-se estabelecer procedimentos para o gerenciamento seguro de credenciais de usuário, incluindo a distribuição, armazenamento e revogação de credenciais quando necessário.

XI. Os sistemas de informação do CHC-UFPR/Ebserh devem ser restritos apenas para acesso interno da instituição. Qualquer necessidade excepcional de disponibilizar uma aplicação para acesso externo, deve ser comunicada ao Comitê de Segurança da Informação (CSI) para avaliação e deliberação.

XII. É de responsabilidade do usuário a proteção do sigilo de suas senhas de acesso a fim de evitar a utilização por outrem, cabendo a responsabilização civil e/ou criminal do mesmo pelos danos cometidos através da má utilização do recurso.

XIII. Todos os acessos aos recursos de informação, incluindo, mas não se limitando a computadores, impressoras, e-mails, sistemas e à Internet deverão ser realizados garantindo a identificabilidade e autenticidade do utilizador, ou seja, mediante a utilização de credenciais de acesso.

a) acessos através de credenciais genéricas devem ser viabilizados apenas em casos excepcionais, solicitados mediante formalização fundamentada, via SEI remetido à Unidade de Infraestrutura, Suporte e Segurança de Tecnologia da Informação (UISTI), com assinatura do gestor da unidade funcional ao qual a credencial estará vinculada;

b) caberá à UISTI a avaliação técnica da necessidade e viabilidade, propondo alternativas sempre que possível bem como a guarda das informações de requisição e vinculação das credenciais;

c) cabe ao Comitê de Segurança da Informação (CSI) monitorar, quando necessário, a adequada instrução das solicitações e dirimir eventuais questionamentos.

Art. 5º Sobre os **crachás de identificação**:

I. É obrigatório para todos os colaboradores, visitantes e prestadores de serviços o uso de crachás de identificação durante todo o período de permanência nas dependências do CHC-UFPR/Ebserh.

II. A emissão, controle e recolhimento dos crachás são de responsabilidade da Unidade de Serviços Gerais (USG), em conformidade com as políticas internas estabelecidas.

III. O uso visível e adequado dos crachás é essencial para garantir a identificação de indivíduos autorizados no ambiente institucional.

IV. Os crachás de identificação deverão ser utilizados para restringir/permitir acesso a recursos, como por exemplo, impressoras e à entrada em áreas sensíveis, direcionadas apenas à pessoal autorizado.

V. É terminantemente proibido o empréstimo do crachá, sendo esse de uso pessoal, exclusivo e intransferível.

VI. Crachás temporários devem ter expiração máxima fixada para até 24 horas e devem ser vinculados ao mínimo de recursos possíveis, não tendo todos os privilégios do permanente.

VII. Crachás provisórios emitidos entre o período de ingresso no CHC-UFPR/Ebserh e a emissão de crachá definitivo podem ter maior prazo de expiração, porém todos os privilégios devem ser revogados tão logo emitido o crachá permanente.

VIII. Nos casos de perda, extravio, furto e roubo, o colaborador deverá comunicar o fato imediatamente à USG, para que sejam tomadas as providências cabíveis.

Art. 6º Sobre a **comunicação institucional**:

I. O uso de e-mails institucionais é a forma oficial de comunicação no CHC-UFPR/Ebserh e deve ser restrito a assuntos relacionados ao trabalho.

II. É proibido o envio de informações confidenciais ou sensíveis por e-mail sem a devida criptografia e autorização prévia da área de origem da informação.

III. Não deve ser redirecionado o e-mail institucional para uma conta pessoal.

IV. Toda mensagem enviada pelo usuário em função na Ebserh deverá conter, ao seu final, a assinatura padrão definida pela empresa.

V. Os usuários devem utilizar as ferramentas de comunicação aprovadas pela instituição, para garantir a integridade e segurança das informações transmitidas.

Art. 7º Em relação ao uso de **redes/mídias sociais** o colaborador deve:

I. Evitar o acesso a qualquer modalidade de mídia social recreativa durante o horário de trabalho.

II. Ser consciente, ao não comentar informações confidenciais da instituição ou assuntos internos tratados em reuniões ou conversas com colegas.

III. Ter responsabilidade sobre as mensagens postadas, não publicando informações enganosas, incorretas ou que prejudiquem a imagem da instituição ou de seus colaboradores.

IV. É vedada a publicação de imagens de pacientes, familiares ou outros sem a devida autorização.

V. Usar a participação nas Mídias Sociais como uma oportunidade para aprender mais e usar os conhecimentos adquiridos para oferecer um serviço de melhor qualidade.

VI. Não divulgar informações sigilosas ou questões internas da empresa ou da vida pessoal de terceiros.

VII. Evitar compartilhar temas que venham a prejudicar pessoas ou grupos de pessoas que representam um determinado estilo de vida ou crença.

Art. 8º Sobre o **armazenamento de informações**:

I. As informações institucionais devem ser armazenadas em sistemas e ferramentas de armazenamentos locais ou na nuvem aprovadas pela área de TI do CHC-UFPR/Ebserh.

II. É estritamente proibido o armazenamento de informações sensíveis ou confidenciais em dispositivos pessoais ou em serviços de nuvem não autorizados.

III. Todos os colaboradores são responsáveis por adotar medidas adequadas para proteger as informações sob sua responsabilidade contra acessos não autorizados, extravio ou divulgação indevida.

IV. Nenhuma informação institucional deverá ser armazenada nos computadores de uso do usuário, uma vez que não são garantidas por cópias de segurança (backups) e estão vulneráveis a acessos indevidos e perdas ocasionadas por problemas no equipamento.

V. Conforme Ofício-Circular - SEI nº 27/2022/SUP/CHC-UFPR-EBSERH, o CHC-UFPR/Ebserh disponibiliza espaço em seus servidores de arquivos, denominado Geral (P:), para armazenamento exclusivamente de dados institucionais, não sendo permitidos em nenhuma hipótese a sua utilização para guarda de arquivos pessoais. Caso arquivos pessoais sejam encontrados neste servidor eles poderão ser excluídos sem aviso prévio.

VI. Todas as informações institucionais deverão ser armazenadas no ambiente de dados compartilhado Geral (P:) ou no ambiente de armazenamento institucional em nuvem (por exemplo: *Onedrive*).

VII. A depender da necessidade e conveniência, os computadores do complexo hospitalar podem ser formatados e é responsabilidade do usuário garantir que as informações sejam sempre salvas em ambientes protegidos e com backups.

VIII. Dados pessoais ou sensíveis não devem ser divulgados em nenhuma pasta do Geral (P:) prefixada com "Todos" (por exemplo "Todos-GAS", "Todos-GAD", "Todos-GEP" ou "Todos-SUP"), pois estas pastas são acessadas por pessoas em todas as unidades funcionais contidas nesta hierarquia.

IX. Para contratações de soluções em nuvem, deve-se seguir as orientações constantes na Norma Operacional SEI nº 6/2022/SGTI/DTI-EBSERH de 21 de novembro de 2022.

X. O acesso e o tratamento de dados pessoais deverão ser protegidos nos termos da Lei nº 13.709, de 14/08/2018, a Lei Geral de Proteção de Dados, bem como dos dispositivos específicos das normas profissionais específicas que regem a proteção de dados dos pacientes, incluindo as limitações de divulgação interna junto a outros colaboradores, bem como a terceiros.

XI. Não devem ser utilizadas unidades portáteis de armazenamento de dados corporativos na Ebserh, devendo ser tratado como exceção à regra, pois são pontos de alta vulnerabilidade de segurança, podendo ser usadas para a fuga de informações corporativas confidenciais.

XII. Quando do uso de unidades portáteis de armazenamento de dados, deve-se prezar pelos princípios da Legalidade, da Razoabilidade, da Ética, devendo ainda serem observados, sem prejuízo dos demais, outros princípios constitucionais que regem a Administração Pública Federal - APF.

Art. 9º Sobre as **disposições finais**:

I. O descumprimento das normas estabelecidas neste documento poderá acarretar medidas disciplinares e administrativas, conforme previsto na legislação interna e nos regulamentos vigentes.

II. A área responsável pela informação é responsável por monitorar o cumprimento deste normativo e propor atualizações conforme necessário, visando sempre a melhoria contínua dos processos de segurança da informação e comunicação.

III. Casos omissos ou não previstos deverão ser direcionados ao Comitê de Segurança da Informação (CSI) mediante processo SEI na caixa CSI/SUP/CHC-UFPR ou por meio do endereço eletrônico: csi.chc-ufpr@ebserh.gov.br.

Art. 10. Esta Norma-SEI entra em vigor na data de sua assinatura.

Aprovado e autorizado por:

(*assinado eletronicamente*)
JANE TERESINHA STIVAL
Gerente de Atenção à Saúde Substituta
do Complexo do Hospital de Clínicas da UFPR

(*assinado eletronicamente*)
PROF. DR. JORGE VINÍCIUS CESTARI FELIX
Gerente de Ensino e Pesquisa do Complexo
do Hospital de Clínicas da UFPR

(*assinado eletronicamente*)
PROF. DR. RAILSON HENNEBERG
Gerente Administrativo do Complexo do
Hospital de Clínicas da UFPR

(*assinado eletronicamente*)
PROF.ª DR.ª CLAUDETE REGGIANI
Superintendente do Complexo do
Hospital de Clínicas da UFPR

Documento assinado eletronicamente por **Claudete Reggiani**, **Superintendente**, em 15/08/2024, às 15:05, conforme horário oficial de Brasília, com fundamento no art. 6º, caput, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Jorge Vinicius Cestari Felix**, **Gerente**, em 15/08/2024, às 15:33, conforme horário oficial de Brasília, com fundamento no art. 6º, caput, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Jane Teresinha Stival**, **Gerente, Substituto(a)**, em 15/08/2024, às 15:49, conforme horário oficial de Brasília, com fundamento no art. 6º, caput, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Railson Henneberg**, **Gerente**, em 16/08/2024, às 11:08, conforme horário oficial de Brasília, com fundamento no art. 6º, caput, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ebserh.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **41589866** e o código CRC **9BE14E56**.

Referência: Processo nº 23759.009589/2024-20 SEI nº 41589866