



SPDM
PAIS

ASSOCIAÇÃO PAULISTA PARA O DESENVOLVIMENTO DA MEDICINA
Fundada em 1933 | Utilidade Pública Municipal, Estadual e Federal | Entidade Filantrópica inscrita no CNAS desde 26/06/1963
Programa de Atenção Integral à Saúde

O CUIDADO COM O SIGILO E A ÉTICA AO LIDAR COM INFORMAÇÕES INSTITUCIONAIS

Informações confidenciais indevidamente divulgadas podem causar danos imensuráveis além de riscos de integridade institucionais, e diariamente carregamos valiosos dados internos e de terceiros, que incluem informações de colaboradores, fornecedores e até mesmo de clientes/usuário. E qualquer deslize pode impactar operações, resultados financeiros e sobretudo nossa reputação institucional.

O cuidado com o sigilo das informações está relacionado também ao acesso não autorizado de colaboradores a dados, é de suma importância saber se as informações que tenho acesso durante as atividades exercidas são consideradas confidenciais, e quem são as pessoas autorizadas para o manuseio, esses dados são considerados ativos importantes e precisam ser protegidos.

É importante a conscientização sobre a responsabilidade no tratamento correto e a ética ao lidar com informações institucionais. Lembrando que o comportamento ético entre os colaboradores de uma instituição garante que o ambiente profissional funcione com honestidade e integridade. Para saber sobre as Regras e Procedimentos Institucionais consulte o [Manual de Conformidade Administrativa, Políticas e Princípios de Integridade da SPDM/PAIS](#).

Pensando nos reflexos positivos listamos algumas boas práticas:

- **Armazenamento de documentos**, após a elaboração de documentos certifique-se que serão devidamente arquivados. Nos casos de arquivos físicos, verifique o local é seguro e se os arquivos estejam devidamente identificados e fora do alcance de terceiros ou pessoas não autorizadas.
- **Em casos de arquivo eletrônico**, garanta que o arquivo seja devidamente salvo em sistemas específicos, plataformas ou ferramentas da própria instituição estabelecido pelo processo, nos quais garanta o acesso aqueles devidamente autorizado.
- **Cuidado ao enviar documentos por e-mail ou malotes**, além seguir a padronização de envio estipulado da instituição, ao enviar, sempre faça a conferência do destinatário, pois podemos enviar informações sigilosas por engano, podendo ocasionar desconforto e até mesmo prejuízos a instituição.



- **E ao receber documento** que não é de sua alçada, informe imediatamente ao remetente e exclua o documento ou devolva ao remetente nos casos de arquivos físicos. Todos os colaboradores têm a obrigação de proteger as informações da intuição e a ciência que documentos ou informações que não compete ao fluxo de trabalho não devem ser compartilhadas ou mantidas na estação de trabalho.
- **Meios de comunicação da Instituição**, a instituição estabelece meios de comunicação oficial para os seus colaboradores. A utilização dos canais oficiais além de ser o meio seguro para o compartilhamento das informações, ela possui rastreabilidade, podendo minimizar e resguardar riscos a exposição ou alterações de registros de formas maliciosas, sendo assim, não recomendamos o uso de outros aplicativos de comunicação. Atenção ao compartilhamento das informações, visto que, o manuseio da informação deve ser feito em plena consciência e cuidado pelo colaborador, atendendo a finalidade do fluxo de trabalho, ou seja, certifique-se que as informações ou documentos compartilhados não ofereçam mais do que o necessário para realização do seu trabalho.
- **Fique atento ao descarte de documentos**, é muito comum o colaborador optar o uso de rascunhos ou bloco de notas com intuito de garantir a prática sustentável, mas certifique-se que o rascunho utilizado não possua informações e dados pessoais de colaboradores, clientes/usuário ou terceiros, faça devidamente o descarte conforme a prática de sustentabilidade da instituição e garanta que o documento seja destruído a ponto de não oferecer exposição de dados pessoais, sensíveis ou sigilosos.
- **Ao se ausentar** de sua estação de trabalho, o colaborador deverá bloquear sua estação de trabalho, seja ele computadores, celulares e afins.
- **Cuidado ao comentar informações**, informações sigilosas e privilegiadas, não devem ser discutidas em ambientes públicos nem compartilhadas com familiares ou amigos.