epihc | ETHICAL PRINCIPLES IN HEALTH CARE™

En colaboración con el
Gobierno de Japón

Resumo do Módulo 7

epihc.org

epihc ETHICAL PRINCIPLES IN HEALTH CARE

In partnership with the Government of Japan

PRINCÍPIO ÉTICO: 7 - PROTEÇÃO DAS INFORMAÇÕES DO PACIENTE

O PORQUÊ, O COMO E O SEU DEVER	APRENDIZADOS-CHAVE, DEVERES E OBRIGAÇÕES CRÍTICAS	SEUS DEVERES E OBRIGAÇÕES
CENÁRIO ACESSO A INFORMAÇÕES PRIVADAS DE CELEBRIDADES	1. Educar e conscientizar continuamente todos os envolvidos sobre os riscos de proteção, especialmente aqueles decorrentes do vazamento de e-mails. 2. Informar pacientes, funcionários e outros indivíduos caso seus dados tenham sido violados e compartilhados. 3. Agir com honestidade e responsabilidade, proibindo práticas que prejudiquem os pacientes e lidando com todas as ameaças ou riscos reais ou percebidos aos dados de pacientes, funcionários e clientes com urgência, transparência e sensibilidade. 4. Manter salvaguardas administrativas, técnicas e físicas apropriadas para garantir que: a) Os registros, documentos e relatórios organizacionais — físicos, digitais ou eletrônicos — sejam mantidos precisos, completos e protegidos contra adulteração. b) As informações médicas sejam mantidas em sigilo. c) As informações sejam protegidas contra perda ou uso indevido. d) A confidencialidade dos registros de pacientes, funcionários e clientes seja mantida de acordo com os padrões legais e éticos aplicáveis. e) Os funcionários sejam proibidos de discutir pacientes e suas condições em áreas públicas. f) Os dados não sejam vendidos ou monetizados sem o consentimento daqueles que contribuíram para os dados.	**NOTAS PARA GERENTES** Seguir as boas práticas é inegociável!
CASO JURÍDICO VIOLAÇÃO DE DADOS DE REGISTROS DE PACIENTES	1. Compreender o quadro regulamentar que rege a proteção de dados. 2. Analisar as estruturas de governança, as políticas formais e os procedimentos que apoiam o uso e a proteção de dados e que estejam alinhados com o quadro regulamentar. 3. Avaliar as lacunas nos processos de governança e fazer recomendações sobre como saná-las na proteção de dados e apoiar as melhores práticas de uso, conforme os Princípios de Dados da OMS. 4. Reportar ao Comitê de Riscos do Conselho as áreas de risco significativo, particularmente em relação à violação de dados. 5. Desenvolver protocolos e procedimentos para ataques cibernéticos e vazamentos de dados. 6. Garantir que os serviços ao paciente sigam os mais altos padrões de mecanismos de proteção de dados. 7. Considerar como as diversas partes interessadas, com diferentes tarefas e interesses, influenciam os tipos de violação de dados, seus fatores e impactos finais. 8. Considerar os fatores institucionais que contribuem para a não conformidade organizacional com as medidas de proteção de dados e como os reguladores e as partes interessadas das organizações de saúde podem abordar esses fatores coletivamente. 9. Proteger a propriedade intelectual, incluindo marcas registradas, direitos autorais e patentes, de fornecedores e outras partes interessadas.	**NOTA PARA A EQUIPE EXECUTIVA SÊNIOR E MEMBROS DO CONSELHO** Fingir ignorância não é uma defesa válida!