O Papel da Sociedade Brasileira de Informática em Saúde na Lei Geral de Proteção de Dados Pessoais (LGPD)

Marcelo Lúcio da Silva
Diretor Executivo da Sociedade Brasileira de Informática em Saúde (SBIS)
Presidente da Federação Latino-Americana de Informática em Saúde (IMIA-LAC)

Apresentação à Comissão Mista da Medida Provisória nº 869/2018
Brasília, 17 de abril de 2019

A SBIS

- Sociedade científica voltada ao desenvolvimento da Saúde Digital no Brasil
- Instituição sem fins lucrativos
- Fundada em 1986, possui atualmente mais de 1.500 membros
- Representante brasileira junto à IMIA – International Medical Informatics Association
- Congrega os profissionais que têm relação ou interesse com a Informática em Saúde

A SBIS

- Missão:

  Melhorar a Saúde por meio do uso adequado das Tecnologias de Informação e Comunicação

- Visão:

  Ser o catalisador do potencial transformador da Informática em Saúde

- Valores:

  Imparcialidade

  Excelência

  Comprometimento

  Diversidade

  Ética

  Entusiasmo

A SBIS

- Mais importante fórum de discussão de Tecnologia da Informação e Comunicação (TIC) em Saúde da América Latina

- Representantes da academia, profissionais e empresas, dos setores público e privado

- Forte colaboração formal e informal com o Ministério da Saúde, Conselho Federal de Medicina (CFM), Associação Paulista de Medicina (APM), Instituto HL7, Associação Brasileira de Normas Técnicas (ABNT) e Sociedade Brasileira de Computação (SBC), entre outros

A SBIS

- Realiza bienalmente o Congresso Brasileiro de Informática em Saúde
- Realizou o Congresso Mundial de Informática em Saúde (MEDINFO) no Brasil em 2015
- Elaborou e executa a Certificação SBIS-CFM para Sistemas de Registro Eletrônico em Saúde (S-RES) desde 2002
- Elaborou e executa o Programa de Profissionalização em TIC em Saúde (proTICS) desde 2011
- Certifica profissionais em TIC em Saúde (cpTICS) desde 2012
- Publica o Journal of Health Informatics (JHI) desde 2009

A Informação de Saúde

- É sensível, já que sua divulgação pode afetar diretamente vida (honra, intimidade) do indivíduo
- Diferentemente de uma transação, ela tem utilidade por toda a vida (e até após)
- É criada, acessada e processada por inúmeras instituições, públicas e privadas (laboratório, atenção primária, consultórios, hospitais, academias, empregadores, planos de saude, ministério da saude, INSS, forças armadas, universidades, institutos de pesquisa e outras), com estruturas de todos os tamanhos e capacidades
- Inclui TODOS os cidadãos brasileiros (100% da população) desde o nascimento à morte, e ainda inclui os estrangeiros no país

A Informação de Saúde

- Rede de mais de 330 mil estabelecimentos
- 165 mil consultórios
- 60 mil clínicas
- 42 mil UBS (somente a metade com alguma informatização)
- 25 mil laboratórios
- 7 mil hospitais
- 1 mil operadoras de planos de saúde
- Mais de 3 milhões de profissionais de saúde, mais de 10 conselhos profissionais
- Mais variados níveis de maturidade em segurança e privacidade

Objetivos quanto à LGPD

- Contribuir com os poderes Legislativo e Executivo na **regulamentação** e **implementação** da LGPD para a área da Saúde

- Auxiliar as **instituições** (hospitais, clínicas, laboratórios, operadoras, etc) e **profissionais** de Saúde a atingir e manter a **conformidade** à LGPD

Ações

- Criada uma comissão especial de trabalho para a LGPD na Saúde
- Elaboração do Manual de Boas Práticas
- Pesquisa do nível de maturidade do setor
- Desenvolvimento de processo de avaliação de conformidade
- Pleito de participação como entidade científica no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (Art. 58-A, VIII da LGPD)

Manual LGPD na Saúde

- Desenvolvimento do Manual de Boas Práticas
  - Específico para o setor de saúde
    - Hospitais
    - Laboratórios
    - Clínicas
    - Operadoras
    - Profissionais de Saúde
  - Auditável
  - Validado em Consulta Pública

Atividades complementares

- Palestras e eventos de conscientização
  - Envolvimento multidisciplinar nas instituições
    - Gestores (desde a alta direção)
    - Profissionais de saúde, TI, administrativo, jurídico, marketing, financeiro e compliance
- Disponibilização de informações, toolkits e pesquisas
- Treinamentos para os Encarregados (Art. 41 da LGPD) da área da Saúde

Em andamento

- COPISS / ANS
  - Padronização de Biometria facial para identificação do beneficiário
- ISO e ABNT já possui normas para:
  - Pseudonimização (ISO 25237:2017)
  - Treinamento em privacidade (ISO/TR 18638:2017)
  - Propósito de uso (ISO/TS 14265:2011)
  - Segurança da informação (ISO 27799:2016)

Certificação SBIS para S-RES

- Manual da SBIS
  - Já possui requisitos recomendados de privacidade
  - **NGS1.12 – Privacidade**
    - NGS1.12.01 Concordância com termos de uso
    - NGS1.12.02 Consentimento do sujeito da atenção
    - NGS1.12.03 Associação do consentimento à informação de saúde
    - NGS1.12.04 Acesso de emergência
    - NGS1.12.05 Propósito de uso

Pontos a Analisar

- O tratamento de dados poderá ser realizado (Art. 7º), sem necessidade de consentimento (inciso I), para:
  - **Proteção da vida** ou da **incolumidade** física do titular ou de terceiro (inciso VII)
  - **Tutela da saúde**, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias (inciso VIII)

Pontos a Analisar

- Art. 11, § 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses de:
  - I - Portabilidade de dados quando consentido pelo titular; ou
  - II - Necessidade de comunicação para a **adequada prestação de serviços de saúde suplementar**

Pontos a Analisar

- Art. 18 O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
  - V - **portabilidade** dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a **regulamentação do órgão controlador**

Pontos a Analisar

- Definição da multa em caso de incidentes (Art. 52)
  - A ANPD dimensionará a multa analisando se a instituição seguiu as melhores práticas em proteção de dados
  - Caso a saúde não tenha uma referência própria, ela se baseará na literatura e nas implementações disponíveis, que remetem largamente ao sistema financeiro
- Ampliação do prazo de adequação de forma escalonada, com o avanço da maturidade do mercado
- Controles diferenciados para portes distintintos (como exemplo, a GDPR diferencia empresas com até 250 funcionários)

Obrigado!

Marcelo Lúcio da Silva

marcelo.silva@sbis.org.br