平成 24 年 7 月 23 日

医療等分野における個別法に関する意見

東京工業大学　社会情報流通基盤研究センター　大山永昭

1. 医療等個人情報の利用シーンの大別
   - 医療等個人情報を参照・提供する利用シーンを、以下の３つに大別する

   １）PHR、EHR、EMR を含む個人情報の参照・提供

   ２）症例データベース等を用いた類似症例の検索

   ３）DB マイニング等による疫学や新たな知見獲得等を目的とした医学研究

2. K-匿名性（K-anonymity）の概念の拡張について
   - 任意の個人データセットを用いて、対象となる多人数 DB の検索を考える
   - この時、与えられた個人のデータセットの項目および各データを自由にマスクし、ヒットする人数を求め、その最小値を K（≧１）と定義　⇒　拡張された K-anonymity と定義
   - 言い換えると、K-anonymity である DB は、最低限 K 人を区別できない DB であることがわかる。
   - したがって、個人を特定できる個人情報は K=1 となる

3. 既存の個人情報保護法について
   - 現在の個人情報保護法では、個人を特定できる情報（K＝１）に関して、その安全な保護・管理を実施すべき旨を規定している
   - また、5000 件以上の個人情報を取り扱う事業者については、安全管理等に不備があると、勧告、次に罰金を事業者に科すこととしている
   - 言い換えると、K＞１の DB については、明確に述べていない

4. 医療分野の DB と K の関係
   - 上記 2.で示した利用シーンに用いられる DB を考える

   １）PHR、EHR、EMR 等の DB は、対象を特定するため K＝１

   ２）症例 DB 等は珍しい症例を含むため K≧1
      - K=1 データが含まれる以上は、アクセス者に対する制限を設ける（公開ではない）べき
      - アクセスできる者については、登録制とするか、資格審査の導入か？

   ３）DB マイニングについて
      - 一般的に K が大きくなるにつれて、その有用性は小さくなる。
      - マイニング対象となる DB が、公開か条件付き開示かで、取り扱いは大きく変わる。
      - 公開であれば、K＞ｎのｎをどうするかが課題。例）ｎ＝10
      - 条件付き開示（ｎ≧K≧１）であれば、開示先の安全・管理レベルに依存することになる。
      - 開示先から DB が漏洩した場合は、開示先の管理責任になる。提供元は、免責か？委託は要注意！
      - 適切な K を定めることができるか？

5. 情報項目の機微性について
   - 医療等個人情報には、病名に代表されるような機微性の高い情報項目も存在している
   - 各情報項目の機微性について、客観的に分類することが可能か？
   - 情報主体者がその機微性を判断する「主観説」を取るとした場合には、全ての項目の機微性が高くなる可能性が生じる。
   - この場合には、項目ごとの機微性に関する議論は不要となるが、他方で保護対策を強化すべきとなる。
   - したがって、情報項目の機微性の議論ではなく、与えられた情報項目の K 匿名性に依存する。言うまでもなく、K=1 は、十分な安全・管理の対象データ。

6. マイナンバー法との対比（参考）
   - マイナンバー法では、マイナンバーが広く知られることから、マイナンバーと個人の属性をつないだ情報を特定個人情報と定義
   - 法案で許可された目的以外は、特定個人情報（K=1）の提供、収集は、本人同意があっても禁止されている　⇒　本人同意による提供、収集は、医療分野では、目的または分野限定による除外とするか。その他の違反者には直罰か？

7. 管理責任と結果責任
   - 現在の個人情報保護法およびマイナンバー法案においては、個人情報の漏洩等の問題発生を避け、その安全管理の重要性を明確にするため、管理責任は事業者にあるとしている。
   - 医師等に科されている守秘義務と刑罰は、秘密漏洩等が生じた際の結果責任に関する規定であり、具体的な被害に対する賠償等については、民事裁判に委ねることとなる。
   - 本規定により、管理責任は結果責任を避けるための予防策として、その実効性が担保されると期待されている。
   - 例えば A さんが、大切なものを管理していると想定する。そして、A さんが管理・保管場所に鍵を掛けずに外出し、泥棒にそのものを奪われたとする。
   - この場合、言うまでもなく泥棒には窃盗罪が適応されるが、同時に A さんの管理責任も問われることになる。
   - しかしながら、医療等個人情報の機微性を勘案すると、今回の個別法では、漏洩等の予防策（具体的には組織及び技術的な対策の履行）の重要性を明確にするため、管理責任に対する何らかの規定を設けることが必要ではないか
   - もちろん、守秘義務等の結果責任が及ばないコ・メディカルの人たちに対する結果責任の規定についても検討すべきであろう

8. 残された課題の例
   - K=1 の医療等分野における個人情報に対する保護は、特定個人情報と同じ範疇になるか？
   - 論点は、マイナンバーのように広く知られていると見なすかどうか。
   - マイナンバーと同じように、広く知られる可能性が高い、いわゆる見える個人番号を医療等分野に導入するならば、本人同意の扱い等に注意を要する。
   - DB の管理責任を、K=1 と K≠１（開示と公表）で分けることの検討が必要。

以上