TTA Technical Report

기술보고서

TTAR-xx.xxxx 제정일: 2018년 xx월 xx일

개인의료정보의 비식별화

De-Identification of Personal Health Information

한국정보통신기술협회
Telecommunications Technology Association

	성명	소 속	직위	위원회 및 직위	표준번호
표준초안 검토 위원회	바이오인식 프로젝트그룹(PG505)				
표준안 심의 위원회	정보보호 기술위원회(TC5)				
표준(과제) 제안	이병기	삼성의료원	교수	-	
	김순석	한라대학교	교수	-	
표준 초안 작성자	김순석	한라대학교	교수	-	
	한태화	연세대학교	교수	-	
	황인정	명지병원	책임연구원	-	
표준 초안 에디터	이병기	삼성의료원	교수	-	
	최민용	BSI Korea	실장	-	
	한근희	건국대학교	교수	-	
표준 초안 검토	김재성	KISA	수석	PG505 의장	
	전동훈	슈프리마	팀장	PG505 부의장	
	전명근	충북대	교수	PG505 부의장	
	한승진	경인여대	교수	PG505 간사	
	김학일	인하대	교수	PG505 특별위원	
	이필중	포항공대	교수	PG505 특별위원	
	정창신	TTA	팀장	PG505 위원	
사무국 담당	김재웅	TTA	단장	-	
	문서연	TTA	전임	-	

발행인 : 한국정보통신기술협회 회장
발행처 : 한국정보통신기술협회
13591, 경기도 성남시 분당구 분당로 47
Tel : 031-724-0114, Fax : 031-724-0109
발행일 : 2018.08

서 문

1 기술보고서의 목적

본 기술보고서는 의료현장을 포함, 각 기관 또는 기업들이 보유하고 있는 다양한 개인의료정보의 비식별화에 관련된 이슈와 용어를 소개하는 데 그 목적이 있다. 본 기술보고서는 비식별화와 재식별에 관련된 지금까지의 주요 간행물을 요약하고 있으나, 비식별화의 적절성이나 특정한 비식별화 알고리즘에 관한 권고를 제시하지는 않는다. 본 기술보고서는 연구자와 학계를 대상으로 개인정보의 비식별화에 관한 기술적 이슈를 제한적으로 제시한다는 목적도 있다. 본 기술보고서는 미국 국가표준기술연구소(NIST)에서 발행된 비식별화 관련 정책과 이슈들을 소개한 것으로 국내에 적용할 경우 분석과 재평가를 통해 국내 환경에 보다 적합하도록 참조하여 사용하길 바란다. 본 보고서는 정보시스템 보안 기술에 대한 높은 수준의 지식을 가진 독자를 염두에 두고 있지만, 더 폭넓은 대중이 접근할 수 있도록 하고 있다.

2 주요 내용 요약

비식별화는 정보 집합에서 식별정보를 제거함으로써 개인정보를 특정한 인물과 연결할 수 없도록 하는 것을 말한다. 이러한 비식별화를 통해 개인정보의 수집, 처리, 기록, 배포, 간행에 관련된 프라이버시 위험을 줄일 수 있다. 그러므로 비식별화는 프라이버시를 보호하면서 개인정보를 이용하고 공유한다는 상반되는 목표 간에 절충점을 찾고자 한다. 지난 2016년 행정안전부 등 정부부처합동으로 발간한 개인정보 비식별조치 가이드라인을 비롯 미국 등 외국의 몇몇 법규와 정책은 개인정보를 공유하기 전에 반드시 비식별화할 것을 규정하고 있다. 또한 구조화된 정보, 자유로운 형식의 문서, 멀티미디어, 의학 영상 등 다양한 종류의 정보를 비식별화할 수 있다. 최근 연구에 따르면, 일부 비식별화된 개인정보를 재식별할 수도 있다. 본 기술보고서는 지난 20년 동안 이루어진 비식별화 관련 연구를 요약하고, 현재의 실태에 관하여 논의하며 향후의 연구과제를 제시하고 있다.

3 인용 기술보고서와의 비교

3.1 인용 기술보고서와의 관련성

본 기술보고서는 미국 국가표준기술연구소(NIST, National Institute of Standards and Technology)에서 발행한 문서(NIST IR 8053 De-Identification of Personal Information)를 준용하여 개인정보를 포함하고 있는 정보의 생성, 사용, 기록, 공유에 관련된 실무적 사안이나 정책적 사안에 관심을 가진 관리, 시민단체, 연구자, 학계, 기타 커뮤니티의 구성원을 대상으로 비식별화와 관련한 정책과 기술적 이슈들에 대해 소개한다.

3.2 인용 표준과 본 기술보고서의 비교표

국가표준기술연구소(NIST) IR 8053	본 기술보고서	비고
NIST IR 8053 De-Identification of Personal Information	개인정보의 비식별화	- 기술보고서 형식에 의한 편집

Preface

1 Purpose

The purpose of this technical report is to introduce issues and terminology related to the de-identification of various personal health information held by each institution or company, including the medical field. This Technical Report summarizes the main publications up to date related to de-identification and re-identification, but does not provide recommendations on the suitability of de-identification or specific de-identification processing algorithms. The purpose of this technical report is to limit the technical issues related to the de-identification of personal information to researchers and academics. This technical report is an introduction to de-identification related policies and issues by the National Institute of Standards and Technology (NIST). When applied in Korea, it should be analyzed and reassessed to better refer to it in the domestic environment. This report is designed with readers with a high level of knowledge of information system security technologies in mind, but it allows access to a wider public.

2 Summary

De-identification refers to the inability to associate personal health information with a particular person by removing identification information from the information set. Such de-identification can reduce the privacy risk associated with the collection, processing, recording, distribution and publication of personal information. Therefore, de-identification seeks compromises between conflicting goals of using and sharing personal information while protecting privacy. Some of the laws and policies of foreign countries such as the United States, including guidelines on personal information de-identification measures published jointly by the government ministries such as the Ministry of the Interior and Safety(MOIS) in 2016, require that de-identification be done before sharing personal information. In addition, various types of information such as structured information, free-form documents, multimedia, and medical images can be unidentified. According to recent studies, some de-identified personal information may be re-identified. This technical report summarizes the studies of the de-identification treatments over the past 20 years, discusses the current situation and presents future research projects.

3 Comparison with Reference Standards

3.1 Relationship with Reference Standards

This technical report conforms to *NIST IR 8053 De-Identification of Personal Information* issued by the National Institute of Standards and Technology (NIST) and introduces policies and technical issues related to de-identification

3.2 Correspondence between this Standard and Reference Standards

This technical report is developed based on NISP IR 8053 with reference to the international standardization status and consideration of the domestic environments.

목 차

개인의료정보의 비식별화
De-Identification of Personal Health Information

1 적용 범위

본 기술보고서는 의료현장을 포함, 각 기관 또는 기업들이 보유하고 있는 다양한 개인의료정보의 비식별화에 관련된 이슈와 용어를 소개하는 데 그 목적이 있다. 본 기술보고서는 비식별화와 재식별에 관련된 지금까지의 주요 간행물을 요약하고 있으나, 비식별화의 적절성이나 특정한 비식별화 알고리즘에 관한 권고를 제시하지는 않는다. 본 기술보고서는 개인의료정보를 포함하고 있는 정보의 생성, 사용, 기록, 공유에 관련된 실무적 사안이나 정책적 사안에 관심을 가진 관리, 시민단체, 연구자, 학계, 기타 커뮤니티의 구성원을 대상으로 한다. 또한 연구자와 학계를 대상으로 개인의료정보의 비식별화에 관한 기술적 이슈를 제한적으로 제시한다는 목적도 있다. 본 기술보고서는 정보시스템 보안 기술에 대한 높은 수준의 지식을 가진 독자를 염두에 두고 있지만, 더 폭넓은 대중이 접근할 수 있도록 하고 있다. 본 기술보고서는 미국 국가표준기술연구소(NIST)에서 발행된 비식별화 관련 정책과 이슈들을 소개한 것으로 국내에 적용할 경우 분석과 재평가를 통해 국내 환경에 보다 적합하도록 참조하여 사용하길 바란다.

2 인용 표준

- NIST SP IR 8053 De-Identification of Personal Information

3 용어정의

3.1 비식별화(de-identification), 가명화(pseudonymization), 익명화(anonymization)

일부 저자와 간행물은 비식별화와 익명화를 혼동하여 사용하고 있다. 일부는 비식별화를 어떤 과정을 표현하는데 사용하고, 익명화는 되돌릴 수 없는 특정한 종류의 비식별화를 지칭하는데 사용하고 있다. 의료에 관련된 특정한 상황에서는 비식별화와 가명화를 동등하게 취급하고 있으며, 정보주체의 신원에 대응하는 가명이 제거되었음을 표현하기 위해 익명화라는 용어를 사용하고 있다.

의학 영상의 경우, 비식별화라는 용어는 실제 환자 식별자(real patient identifier)를 제거하는 과정, 또는 익명처리를 위해 영상 개인정보에서 모든 정보주체 집단을 제거하는 과정을 가리킨다. 한편, 비인격화(de-personalization)라는 용어는 임상시험 식별자를 포함하여, 영상에서 정보주체와 관련된 모든 정보를 완전히 제거하는 과정을 의미한다.

따라서 익명화라는 용어의 용법과 정의가 일관되지 않기 때문에 본 기술보고서에서는 되도록 익명화라는 용어를 사용하지 않는다. 대신에 본 보고서에서는 비식별화된 정보를 재식별할 수 있거나 그렇지 않을 수도 있음을 감안하여 비식별화라는 용어를 사용한다.

3.2 개인적으로 식별 가능한 정보(Personally Identifiable Information, PII) 및 개인 정보 (Personal Information)

비록 다양한 법규와 기관의 지침에 개인적으로 식별 가능한 정보(PII)라는 용어에 관한 다양한 정의가 있지만, 이 용어는 보통 개인에 대한 특정한 식별자를 포함하고 있는 정보를 지칭한다. 다양한 정의가 있기 때문에, 특정인을 식별하지만 PII에 관한 정의에 부합되지 않는 정보가 있을 수 있다. 어떤 문서에서는 PII라는 용어를 개인에게 귀속되는 정보 또는 특정한 개인에게만 귀속시킬 수 있는 정보를 지칭하는 반면, 다른 문서에서는 이 용어를 사실 상, 개인을 식별하고 있는 정보에만 사용하고 있다.
이렇게 일관성이 없기 때문에, 이 문서에서는 개인적으로 식별 가능한 정보라는 용어의 사용을 자제한다. 대신에 개인정보(personal information)라는 용어를 이용하여 개인에게서 나온 정보를 지칭하며, 개인을 식별하는 정보는 식별정보(identifying information)라는 용어를 사용한다. 따라서 식별정보는 개인정보이지만 개인정보는 식별정보가 아닐 수도 있다.

4 약어

- PHI : Personal Health Information
- PII : Personally Identifiable Information

5 비식별, 재식별, 정보 공유 모델

본 장에서는 비식별화의 이유를 설명하고 그 효과를 알아보기 위해 재식별 공격에 관해 논의하며, 식별한 개인정보를 공유하기 위한 모델에 관하여 설명한다.

5.1 비식별화의 필요성

개인정보를 수집하고 유지하는 기관들은 한편으로는 개인정보를 최대한 광범위하게 사용하고 공유하면서, 다른 한편으로는 개인정보를 보호해야 하는 어려움이 점점 가중되고 있다. 정부 정보는 공유를 통해 투명성을 높이고 민간 기업에 새로운 자원을 제공하며, 전반적으로 효율적인 정부가 될 수 있다. 민간 기업들은 공개성과 시민 참여의 확대라는 형태로 공유되는 정보에서 이익을 실현하고, 심지어는 개인정보 판매나 분석 결과에서 이익을 얻을 수도 있다.
개인정보에 예를 들면 성명, 이메일 주소, 지리적 위치정보 또는 사진 등의 식별정보가 들어 있는 경우, 개인정보의 사용과 프라이버시 보호라는 목표 간에 갈등이 있을 수 있다. 이러한 갈등을 해결하기 위한 비식별화를 통해, 다른 유용한 정보는 남겨두고 개인을 식별하는 일부 프라이버시에 관련된 민감한 개인정보를 제거할 수 있게 된다.
그러므로 비식별화는 기관들이 개인정보를 포함하고 있는 정보를 생성, 사용, 기록, 공유, 심지어 간행하는 것에 관련된 프라이버시 위험을 최소화할 수 있는 중요한 도구이다. 수집 당시 또는 최소한의 처리를 한 이후에 개인정보를 비식별화하면, 의도하지 않은 공개(즉, 개인정보 침해)에 관련된 프라이버시 위험을 줄임으로써 개인정보를 사용하고 기록으로 보존하는 비용을 줄일 수 있다. 비식별화된 정보를 공유하면 기술적 통제와 정책적 통제 수요가 줄어들 수 있다. 그러므로 기관들은 비식별화를 통해 개인정보를 더욱 잘 활용할 수 있다.
미국의 몇몇 법규는 개인정보 비식별화의 중요성과 효용을 특별히 인식하고 있다. 다음과 같은 예가 있으나 이에 한정되지는 않는다.

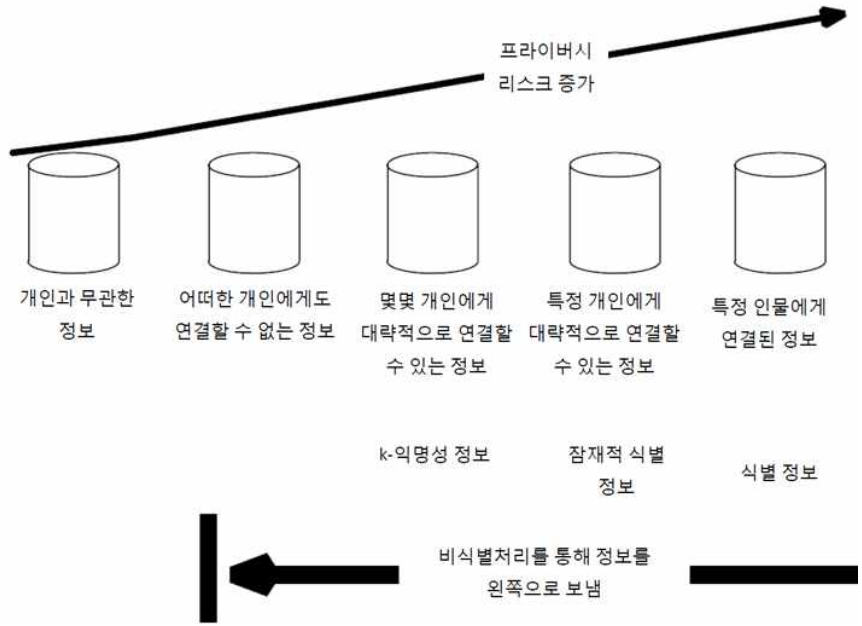
- 교육부는 「가족 및 교육 개인기록부 프라이버시 법(the Family and Educational Records Privacy Act, FERPA)」에 따른 제한이 비식별화된 학생 개인기록부에는 적용되지 않는다는 입장을 취하고 있다. '교육관련 정부기관과 교육기관은 개인적으로 식별 가능한 모든 정보를 제거함으로써, 비식별화된 교육 개인기록부 또는 교육 개인기록부에 있는 개인정보를 동의 없이 공개할 수 있다.'
- 「의료보험의 이동과 책임에 관한 법률(Health Insurance Portability and Accountability Act, HIPAA)」 프라이버시 규칙과 「경제와 임상보건을 위한 의료정보기술 법(the Health Information Technology for Economic and Clinical Health Act, HITECH)」은 '해당 정보를 이용하여 개인을 식별할 수 있다고 믿을만한 합리적인 사유가 없는' 경우, 비식별화된 의료 정보에는 명시적으로 적용되지 않는다.
- 질병 통제 및 예방본부(the Centers for Disease Control and Prevention)가 운영하는 식품유래 질병 감시체계(the Foodborne Illness Surveillance System)에 따르면, '종합되고 비식별화된 감시 개인정보에 대한 적시적인 일반인의 접근(access)'을 허용해야 한다.
- 미국 보건복지부와 계약을 체결하여 약품안전 정보를 제공하는 업체들은 그러한 정보를 비식별화된 형태로 제공할 능력이 있어야 한다.
- 미국 연방항공국(the Federal Aviation Administration)에 제출되는 자발적 안전 보고서는 만약 보고서에 담긴 개인정보가 비식별화되었다면 대중에 공개할 수 있다.

이러한 법규는 개인정보를 제거하고 나머지 개인정보를 정보주체의 신원을 공개하지 않는 식으로 사용할 수 있도록 하여, 비식별화를 개인정보에 적용할 수 있는 기술적 통제 수단으로 간주한다. 그러나 데이터베이스에 있는 특정 항목을 범주화(suppressing)하거나 일반화(generalizing)하는 비식별화 접근방식은 프라이버시에 대한 절대적인 보장 수단이 될 수 없다. 왜냐하면 보조 정보 집합을 이용하여 나머지 개인정보를 재식별할 수 있는 가능성이 항상 있기 때문이다. 6.6절에는 적절히 비식별화된 것으로 간주되었던 개인정보가 공개되었고, 나중에 연구자나 언론이 이를 재식별한 유명한 몇 가지 사례를 논의하고 있다. 이러한 재식별 사례 중 일부에서는 정보주체의 신원을 노출시켰다. 정보집합을 신원에 연결하였던 특정한 속성을 공개함으로써 발생할 수 있는 프라이버시에 관련된 이슈도 있다. 그럼에도 불구하고 HIPAA 비식별화 기준(특정 항목의 범주화를 기초로 함)을 충족시킬 수 있는 두 가지 접근법 가운데 하나인 HIPAA '세이프 하버(Safe Harbor)' 방식을 통한 시험에 따르면, 남은 식별 정보가 출생연도, 성별, 3자리 우편번호

(Zip code)뿐인 경우에는 비식별화된 개인기록부 중에 재식별할 수 있는 부분은 1% 미만이라는 사실이 밝혀졌다(6.5절 참조).

재식별이라는 위험이 있기 때문에 비식별화된 개인정보를 공유하는 일부 기관들은 정보 이용자들과 정보 이용에 관한 합의서(data use agreement, DUA)를 체결하려 할 수 있다. 예를 들면 DUA를 체결함으로써, 비식별화된 개인정보의 이용자가 정보주체를 재식별하려 하거나 외부 정보와 연결하거나 무단으로 개인정보를 공유하는 행위를 막을 수 있다.

(그림 1)에 제시된 것처럼, 식별가능성을 기준으로 모든 개인정보를 분류할 수 있다. 왼쪽 끝에 있는 개인정보는 개인에 관련된 정보가 아니기 때문에(예를 들면 과거의 날씨 기록) 프라이버시에 관련된 위험이 없다. 오른쪽 끝에 있는 개인정보는 특정인에게 직접 연결되어 있다. 이러한 양쪽 극단의 중간에는 노력을 통해 연결할 수 있는 개인정보, 집단에만 연결할 수 있는 개인정보, 개인을 기반으로 한 정보이지만 역으로 연결할 수 없는 정보가 있다. 일반적으로 보면, 비식별화라는 접근방식은 필요한 효용성을 유지하면서 개인정보를 왼쪽으로 밀어냄으로써, 비식별화된 개인정보를 광범위한 집단이나 일반 대중에게 배포할 위험을 낮추도록 하는 방식이라고 할 수 있다.



(그림 1) 개인정보 식별 가능성 스펙트럼

프라이버시를 옹호하는 사람들은 공정정보원칙(Fair Information Practice Principles, FIPP)에 따라, 설령 공유하는 개인정보를 비식별화하더라도, 그리고 정보주체에게 통지해

야 할 법적 의무는 없지만, 정보주체에게 그들의 개인정보가 공유될 것이라는 사실을 통지해야 한다는 입장이다. 그러나 미국의 현행 정책과 법률은 기관들이 이용하는 비식별화된 개인정보의 용도에 대해 상당한 자유를 부여하고 있다. 이러한 정책들은 일반적으로 비식별화된 개인정보를 사용함으로써 유발되는 사회적 편익과 개인정보의 재식별에서 유발될 수 있는 정보주체에 대한 인지된 위험 사이에 균형을 맞추기 위한 정책이다. 기술이 발전함에 따라 이러한 위험이 변할 수 있기 때문에, 비식별화된 개인정보의 사용에 관한 정책을 주기적으로 검토하는 것이 중요하다.

5.2 프라이버시 보존형 개인정보보호 모델

학계에서는 정보주체의 프라이버시를 보호하면서 데이터베이스에 있는 개인정보를 이용하기위한 두 가지 모델을 두고있다.

- 프라이버시 보존형 데이터 마이닝(Privacy Preserving Data Mining, PPDM). 이 모델에서는 개인정보가 공개되지 않으며, 대신에 통계적 처리나 기계 학습(machine learning)에 사용된다. 계산 결과는 기계 학습 알고리즘을 이행하는 요약화(summarization), 총계처리(aggregation), 분류자(classifier)를 기초로 한 통계표의 형태나 및 다른 형태의 결과로 공개할 수 있다.
- 프라이버시 보존형 데이터 간행(Privacy Preserving Data Publishing, PPDP). 이 모델에서는 개인정보를 처리하여 사용자에게 배포할 수 있는 새로운 비식별화되거나 합성한 정보를 생산한다.

이 두 모델은 모두 원본 정보 집합에 있는 특정인에게 귀속시킬 수 있는 정보를 노출하지 않고 일부 개인정보(예, 총계처리 한 정보, 통계적 결과, 분류자 또는 합성한 개인정보)를 노출하도록 하기 위한 것이기 때문에 '프라이버시 보호' 모델이라 부른다.

5.2.1 프라이버시 보존형 데이터 마이닝(PPDM)

PPDM은 공식 통계를 발표하기 위해 민감한 개인정보를 이용하는 것을 가리키는 일반적인 용어이다. 비밀 설문조사 정보를 요약한 통계 보고서가 그 예라고 할 수 있다.

- 통계적 공개 한도(Statistical Disclosure Limitation)란 "3자가 정보를 이용하여 정보에 있는 개인을 인식하는 것을 방지하기 위해 통계적 정보를 변경하는 원칙이다." 공개 제한을 위해 개발된 기법에는 보고된 정보를 더 큰 범주로 일반화하는 기법, 유사한 개체 간에 정보를 교환하는 기법, 문서에 잡음(noise)을 삽입하는 기법 등이 있다.
- 차분 프라이버시(Differential Privacy)란 정보 집합의 계산에서 비롯되는 신원 공개와 정보 누출에 관한 수학적 정의를 이용하는 기법을 말한다. 차분 프라이버시는 수학적 계산의 결과를 보고하기 전에 비결정적 잡음(non-deterministic noise)(보통 작은 임의 값)을 삽입함으로써 공개를 방지한다. 차분 프라이버시의 수학적 정의에 따르면, 정보 집합의 분석 결과는 한 정보 개인기록부(보통은 단일한 인물의 개인정보로 간주됨)을 추가하거나 제거한 전과 후에 대략적으로 동일해야 한다. 삽입한 잡음이 개인

정보를 마스킹(masking)하기 때문에 효과가 있다. 동일한 정도는 변수 ε(입실론)으로 정의한다. ε값이 작을수록 더 많은 잡음이 첨가되며, 단일 개인정보를 분간하기가 더욱 어려워진다. 결과적으로 정보주체 전체의 프라이버시가 높아진다. 가장 기본적인 형태의 차분 프라이버시는 온라인 문의 시스템에만 적용되지만, 차분 프라이버시를 이용하여 기계 학습 통계 분류자와 합성 정보를 생성할 수도 있다.

현재 차분 프라이버시에 관한 연구가 활발하지만 지금까지는 다음과 같은 몇몇 계산 시스템에만 적용되어왔다.

- 합리적이고 정확한 블록(block) 단위의 합성 인구조사 정보를 생성하기 위해 차분 프라이버시를 이용하고 있는 미국 통계국(the Census Bureau)의 '온더맵(OnTheMap)' 웹사이트
- 사용자의 컴퓨터와 사용자의 홈페이지에서 구동되는 윈도(Windows) 프로세스에 관한 총계 통계를 수집하기 위해 임의화 된 반응을 사용하는 구글(Google)의 '크롬(Chrome)' 웹브라우저. 비록 통계는 총계 수준에서 정확하지만 임의화를 하기 때문에, 사용자의 프로세스나 홈페이지를 신뢰성 있게 확인할 수 없다.

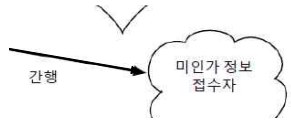
차분 프라이버시를 적용하면 결과의 정확도가 낮아진다. 예를 들면, Fredrikson 등은 임상시험 자료를 이용하여 유전자 정보와 와파린(warfarin) 투여의 상관관계에 관한 통계적 모델을 수립하기 위해 차분 프라이버시를 사용하는 경우에 미치는 영향을 확인하였다. 이 연구는 비록 실제 임상시험이 아니라 시뮬레이션에서만 시험되었지만, 차분 프라이버시를 이용하여 수립한 모델은 차분 프라이버시를 이용하지 않고 수립한 모델에 비해 유의미한 숫자의 환자에게서 더 열악한 임상적 결과가 나오는 경향이 있음을 밝혔다.

5.2.2 프라이버시 보존형 데이터 간행(PPDP)

PPDP를 이용하여 개인정보에 기반한 정보를 간행할 수 있어, 다른 연구자들이 새로운 분석을 할 수 있게 된다. PPDP를 이용하는 목적은 정보주체의 신원을 노출시키지 않으면서도 효용성이 높은 정보를 제공하기 위한 것이다.

- 비식별화는 "식별 정보와 정보주체 간의 연계성을 제거하는 과정을 나타내는 일반적인 용어이다." 비식별화는 개인의 신원을 보호하기 위한 것이며, 다른 목적을 위한 정보 집합의 유용성의 일부를 보존하면서, 정보 집합에 있는 개인정보가 만약 특정 개인에 관련되어 있다면 알기 어렵거나 불가능하도록 한다. 비식별화는 PPDP를 달성하기 위한 주요한 도구이다.
- 합성 정보 생성(synthetic data generation)은 원본 정보와 유사한 정보 집합을 생성하기 위해 PPDM 기법을 일부 이용하지만, 이 때 정보 요소의 일부 또는 전부가 생성되고, 실제 개인을 참조(mapping)하지 않는다. 그렇기 때문에 합성 정보 생성은 PPDM과 PPDP가 융합된 것으로 간주할 수 있다.

5.3 비식별화 정보 흐름 모델



(그림 2) 개인정보 수집, 비식별화 및 이용

(그림 2)에는 비식별화 과정이 기술되어 있다. '정보가 참조하는 사람인' 정보주체(Data Subject)로부터 개인정보를 수집한다(ISO/TS 25237). 이러한 개인정보는 개인정보를 포함하고 있는 정보 집합으로 결합된다. 비식별화를 통해, 식별정보가 없는 것으로 간주되는 새로운 정보 집합을 생성한다. 기관들은 프라이버시 위험을 줄이기 위해 이 정보 집합을 원본 정보 집합 대신에 내부적으로 사용할 수 있다. 이 정보 집합은 데이터이용합의서(DUA) 등의 추가적인 관리적 통제를 받는 신뢰할 수 있는 정보 접수자에게 제공할 수 있다. 그 대신에, 예를 들면 비식별화된 개인정보를 인터넷에 게시함으로써 이 정보를 수많은(아마도 무수한) 미지의 미인가 정보 접수자에게 널리 배포할 수 있다.
(그림 2)에 제시된 대로, 비식별화된 개인정보를 대중에게 공개할 필요는 없다. 더욱이, 비식별화는 정보주체의 신원을 보호하기 위해 적용되는 몇 가지 통제 가운데 하나에 지나지 않을 수 있다.
비식별화는 자동 프로세스, 수작업 또는 이 둘을 혼합하여 수행할 수 있다. 비식별화가 이루어진 경우, 개인정보를 수작업으로 검토하거나 다른 방법을 이용하여 확인함으로써 식별 정보가 남아 있는지, 또는 다른 정보 출처와 연계하여 비교함으로써 제거된 신원을 알 수 있는지 확인할 수 있다.

5.4 재식별 공격 및 정보 공격자

재식별은 비식별화된 개인정보에서 제거된 신원을 분간하려는 과정을 의미한다. 비식별화를 하는 주된 목적은 승인되지 않은 재식별을 방지하는 것이기 때문에 그러한 시도는 종종 재식별 공격(re-identification attack)이라고 부른다.
'공격'이라는 용어는 컴퓨터 보안에 관한 문헌에서 따왔는데, 공격에서는 특수한 기법, 지식, 접근권(access)을 갖고 있는 가상적인 '공격자(attacker)'를 이용하여 컴퓨터 시스템이나 암호화 알고리즘의 보안을 분석한다. 위험 분석에는 잠재적인 공격자를 나열하고 각 공격자의 성공 확률을 분석한다.

개인이나 조직이 재식별 공격을 하는 데에는 많은 이유가 있다.

- 비식별화의 품질을 시험하기 위해 : 예를 들면, 연구자는 정보 처리자(data controller)의 요청에 따라 재식별 공격을 수행할 수 있다. 만약 원본 정보에 개인 보건정보 또는 교육 개인기록부 등의 일종의 법적으로 보호받는 정보가 담겨 있다면, 연구자는 사전에 적절한 비밀준수 합의서를 체결하고 적절한 보안 절차를 시행해야 한다. 그렇지 않을 경우, 재식별의 성공은 '법규 위반(breach)'으로 간주될 것이며, 적용 가능한 법규나 정책에 따라 의무적인 보고 요건이 작동하게 될 것이다.
- 재식별 수행에 관한 대중의 관심 또는 전문가적 관점을 얻기 위해 : 재식별에 성공한 몇몇 사례는 뉴스거리가 되거나 그를 수행한 학자에게 보상이 뒤따랐다. 이러한 공격이 재식별을 금지하는 DUA를 체결하지 않고 합법적으로 수행되었음에 유의한다.
- 비식별화를 수행한 기관을 곤경에 처하게 하거나 해할 목적으로 : 비식별화를 수행하는 기관은 일반적으로 원본 정보에 담긴 개인정보를 보호할 의무를 진다. 그렇기 때문에 부적절한 프라이버시 보호 조치가 적용되었음을 보여줌으로써 이러한 기관을 곤경에 처하게 하거나 해할 수 있다. 특히 비식별화된 개인정보가 공개적으로 유출된 경우에 그러하다.
- 재식별된 개인정보에서 직접적인 이익을 얻기 위해 : 예를 들면, 마케팅 회사는 비식별화된 건강정보를 구입하여 그러한 정보를 신원과 매칭시켜, 재식별된 사람들에게 특정한 처방약 쿠폰을 발송할 수 있다.
- 재식별을 통해 민감한 개인정보를 알 수 있는 사람들에게 곤경이나 해와 같은 문제를 야기하기 위해 : 직접 개인정보를 공개하거나 개인을 위협 또는 비방하기 위해 개인정보를 사용하거나 사임을 강요하거나 다른 부정적인 결과를 강제하기 위해 개인정보를 사용함으로써 문제가 발생할 수 있다.

문헌에 따르면, 재식별 공격은 종종 비식별화된 정보 집합과 약간의 추가적인 배경 정보를 갖고 있는 가상의 정보 공격자(data intruder)가 수행하는 것으로 기술되어 있다(대중에게 공개된 정보 집합의 경우, 정보 공격자는 컴퓨터 시스템이나 정보 집합에 대한 비승인 접근권(unauthorized access)을 획득할 필요가 없다는 점에 주의한다). 재식별 위험(re-identification risk)란 정보 집합에 있는 식별자와 기타 개인에 관련된 정보를 비식별화된 개인정보로부터 알게 되는 위험을 나타내는 척도이다. 재식별 능력은 원본 정보 집합, 비식별화 기법, 공격자의 기술적 능력, 공격자의 가용한 자원, 비식별화된 개인정보에 연결할 수 있는 추가 정보의 가용성에 달라 달라지기 때문에 이러한 위험을 정량화하기는 어렵다.
기법이 개선되고 상황적 정보가 많아짐에 따라(예, 공개 또는 구매를 통해), 재식별 위험이 증가하게 될 것이다. 그렇기 때문에 미래에 재식별에 어떤 종류의 상황적 정보가 활용될 수 있는지를 알고리즘을 이용하여 정하는 것은 불가능하다.
연구자들은 재식별 위험을 계산하고 보고하기 위해 다양한 접근법을 취해 왔다. 그러한 접근법에는 통상적으로 성공 정도를 기술하는 시나리오와 공격자가 갖고 있는 자원과 능력을 측정하기 위한 도구 등이 있다. 재식별 시나리오에는 다음과 같은 예가 있다.

- 만약 특정인이 정보 집합 안에 있음을 공격자가 알고 있는 경우, 그러한 특정인을 재식별할 위험('검사(prosecutor) 시나리오')

- 정보 집합 안에 재식별할 수 있는 사람이 최소한 1명이 있는 위험. 누군가를 재식별할 수 있음을 증명하는 것이 중요하다. 이 경우, 비식별화를 수행한 기관을 곤경에 처하도록 하거나 신뢰를 떨어뜨리는 것이 재식별의 목표인 경우가 많다('기자(journalist) 시나리오').
- 정보 집합 안의 신원의 비율을 정확하게 재식별할 수 있는 경우('마케터(marketer) 시나리오')
- 어떤 개인이 포함된 정보 집합에 대해 수행한 분석과 해당 개인이 포함되지 않은 정보 집합에 대해 수행한 같은 분석 간의 구분 가능성('차분 식별 가능성(differential identifiability)' 시나리오).

정보 공격자의 능력을 기술하기 위해 다음과 같은 기준을 사용한다.
- 공개된 정보에 대한 접근권(access)이 있는 일반 대중('일반 대중')
- 재식별에 숙련된 컴퓨터 과학자('전문가')
- 정보 집합을 생산한 기관의 구성원('내부자')
- 비식별화된 개인정보를 접수하는 기관의 구성원이나, 일반 대중에 비해 더 많은 배경정보에 대한 접근권(access)이 있을 수 있는 사람('내부 접수자')
- 정보를 조합하여 풍부한 정보 상품을 생산하고, 이를 내부적으로 활용하거나 다시 판매할 목적으로 식별된 정보와 비식별화된 정보를 모두 체계적으로 획득하는 정보 브로커('정보 브로커')
- 특수한 상황에 있는 정보주체의 친구 또는 가족('참견하는 이웃')

비식별화를 하는 목적은 정보주체의 신원을 가림으로써 약간의 프라이버시를 보호하면서도 비식별화된 개인정보를 활용할 수 있도록 하는데 있다.
비식별화 정도와 생성된 정보의 유용성 간에 상충 관계가 있다는 점에서 볼 때, 이 두 가지 목표는 상반된 목표이다. 그러나 비식별화를 하면, 과거에는 프라이버시에 대한 우려로 인해 사용이 금지되었던 개인정보를 새롭게 활용할 수 있게 된다. 그러므로 적절한 보안 수준, 따라서 비식별화와 유용성 간에 수용할 수 있는 절충점을 찾는 역할은 정보관리자, 표준기관, 규제기관, 입법자, 법원이 맡는다.
어떤 경우에는 비식별화된 개인정보를 사용함에 따라 정보 집합에 있는 사람에 해가 되거나 프라이버시에 부정적인 행위가 있을 수 있다. 일반적인 분류학에 따르면, 그러한 위험은 신원 공개, 속성 공개, 추론적 공개(inferential disclosure) 등 세 가지로 구분된다.

신원 공개(identity disclosure)는 공격자가 특정한 정보 항목을 특정인에게 연결시킬 수 있을 때 일어난다. 몇 가지 시나리오를 통해 신원 공개가 발생할 수 있다.
- 비식별화가 불충분한 경우 : 통제가 불충분할 때, 비식별화된 정보 집합 안에 의도치 않게 식별정보가 남아있을 수 있다. 2006년에 AOL이 누출한 검색 문의(query) 정보의 경우가 그러하였다. AOL은 약간의 식별 정보를 제거했지만 사용자가 입력한 검색어를 보존하였다. 아라비아 숫자 코드 하나를 통해 정보에서 사용자를 식별하였다. 해당 코드는 임의적으로 생성된 가명(pseudonym)이었기 때문에 자체적으로는 사용

자의 신원에 다시 연계할 수 없었다. 검색 문의 자체에 식별정보가 나타났고(예를 들어 자신의 자산에 관한 정보를 검색한 사람들), 가명이 있었기 때문에 동일한 사용자의 다른 복수의 문의에 매칭시킬 수 있었다. 기자들은 그러한 검색어로부터 몇몇 사용자를 식별할 수 있었고, 사용자와 연락하여 논평을 요청하였다. 다른 사례에서 Sweeney는 워싱턴 주립 병원의 비식별화된 퇴원 개인기록부에 있는 일부 환자의 경우, 퇴원 개인기록부에 있는 정보와 입원을 유발하게 된 사건에 관한 신문 기사를 수작업으로 연관시킴으로써, 환자 정보를 식별할 수 있음을 보여주었다.

- 연결을 통한 재식별 : 남아있는 일부 정보를 다른 식별 정보 집합에 있는 유사한 속성과 연결시킴으로써 특정한 개인기록부를 재식별할 수 있다. 예를 들어, 검색 기록을 비식별화하면 검색자의 성명을 제거할 수 있지만, IP 주소가 남게 되어 해당 정보를 IP 주소를 성명과 연계하는 데이터베이스에 연결할 수 있다.
- 가명 역추적 : 어떤 개인정보를 가명처리하였고, 만약 가명이 신원 정보에서 도출된 것이라면, 가명처리 과정을 역으로 되돌릴 수 있다. 6.2절에 논의된 뉴욕 시 택시 리무진 위원회가 공개한 택시 승차 정보 집합의 경우가 이에 해당한다.
- 속성 공개(attribute disclosure)는 약간의 비밀 정보를 정보주체에 귀속시킬 수 있을 때 발생한다.

정보 집합에 비밀정보가 조금이라도 포함되어있는 경우, 신원이 공개되면 반드시 속성이 공개된다. 그러나 한 정보 집합이 어떤 특징을 공유하고 있는 개인이 특정한 속성을 모두 갖고 있음을 드러내고, 만약 적이 샘플에서 그러한 특성을 갖고 있는 개인을 알고 있는 경우, 신원이 공개되지 않고 속성이 공개될 수 있다. 예를 들면, 한 병원이 치료한 20세 여성 모두가 특정한 진단을 받았음을 나타내는 정보를 공개하고, Alice Smith가 20세 여성이며, 해당 병원에서 치료를 받은 사실이 알려져 있다면, 비록 그녀의 비식별화된 치료 개인기록부를 다른 사람들의 것과 분간할 수 없더라도, Alice Smith의 진단 결과를 추론할 수 있다. l-다양성 기법을 활용하면, 특정한 기준에 일치되는 개인기록부 집단 각각이 일정 수준의 다양성을 갖고 있도록 함으로써 추론적 공개로부터 보호하는데 도움이 될 수 있다. 이러한 접근방식은 심지어 그렇게 할 필요가 없을 경우, 예를 들면 정보주체에 낙인화(stigmatization) 또는 해를 입힐 위험이 없는 경우라도 정보의 유용성을 낮출 수 있기 때문에 적용할 때 신중해야 한다.

- 추론적 공개는 “공개된 정보의 통계적 특징으로부터 높은 신뢰도로 개인정보를 추론할 수 있는 경우에 발생한다. 예를 들면, 어떤 정보는 소득과 주택 구매 가격 간에 높은 상관관계를 나타내고 있을 수 있다. 주택의 구매 가격은 통상적으로 공개되는 정보이기 때문에 제3자는 이 정보를 이용하여 정보주체의 소득을 추론할 수 있다.”

추론적 공개가 발생하는 경우에는 자신의 개인정보가 정보 집합에 포함되어 있지 않은 사람을 포함하여 개인들로 이루어진 전체 계층이 집단적인 해(group harm)를 입을 수 있다. 예를 들면, 어떤 정보 집합에 특정 인구학적 집단이 잘 대표되어 있고, 해당 집단이 정보 집합에서 낙인화되는 비율이 높다면, 비록 해당 인구 집단에 포함된 모든 사람들이 낙인화되는 것이 적절하지는 않지만 그렇게 될 수 있다.

법률과 규정에 반영되어 있는 미국의 프라이버시 정책은 일반적으로 신원 공개를 우려하고 있으며, 식별된 개인정보를 이용하거나 배포하여 발생할 수 있는 기타 해악이나 문제는 우려하지 않고 있다. 이러한 위험을 해결하려는 기관은 명시적 윤리 검토(explicit ethics review)를 통해 그러한 문제를 해결하려 할 수 있다. 그러한 검토는 다음과 같은 내용을 적절히 감안하여 조절해야 한다.

- 해당 기관이 비식별화 절차를 수행하고 시험하는데 투입할 수 있는 노력
- 비식별화된 개인정보를 통한 효용(즉, 해당 정보에 대표된 개인 및/또는 집단에 대한 이익)
- 비식별화된 개인정보를 이용하여 발생할 수 있는 개인 또는 집단의 문제
- 위험을 최소화할 수 있는 다른 통제를 활용할 능력
- 공격자가 개인정보 재식별을 시도할 확률과 공격자가 할 수 있는 노력의 양

5.5 공개 모델과 개인정보 통제

재식별이 발생할 가능성을 줄일 방법에는 개인정보를 획득하고 사용하는 방식을 통제하는 방법이 있다. 이러한 통제는 공개 모델에 따라 분류할 수 있다. 문헌에는 무제한(no restriction)에서 엄격한 제한(tight restriction)에 이르는 몇 가지 모델이 제안되어 있다.

- 일반 공개 모델(the Release and Forget model) : 통상적으로 인터넷에 게시함으로써 비식별화된 개인정보를 대중에 공개할 수 있다. 이러한 방식으로 일단 개인정보가 공개되면 기관이 개인정보를 회수하기는 거의 불가능하다.
- 데이터 이용 합의서(DUA) 모델 : 개인정보를 어떻게 이용할 수 있는가를 세부적으로 규정한 법적 구속력이 있는 데이터 이용 합의서에 따라 비식별화된 개인정보를 공개할 수 있다. 통상적으로 데이터 이용 합의서는 재식별 시도, 다른 정보와의 연결, 정보 재배포를 금지한다. DUA는 개인정보 보유자와 자격을 갖춘 연구자(‘유자격 조사자 모델’) 간에 협상하는 것이 보통이지만 정보를 다운로드하기 전에 합의해야 하는 사용자 클릭(click-through) 라이선스 합의서로 인터넷에 쉽게 게시할 수 있다(‘사용자 클릭 모델’).
- 밀실 모델(the Enclave model) : 비식별화된 개인정보를 원본 정보의 수출(export)을 제한하는 일종의 밀실(enclave)에 유지하고, 대신에 유자격 연구자의 문의를 수락하고 비식별화된 개인정보에 대한 문의를 운영하며 결과를 응답할 수 있다.

프라이버시와 정보 정책 컨설턴트인 Robert Gellman은 데이터 이용 합의서를 보강할 입법안을 제시한 바 있다. Gellman는 그가 잠재적으로 식별 가능한 개인 정보(potentially identifiable personal information, PI)라고 부르는 새로운 정보 범주를 제안한다. 이에 동의하는 당사자는 자신들의 데이터 이용 합의서에서, 해당 정보에서 개인 식별자는 제거되었지만 여전히 재식별될 수 있다는 정보 제공자의 약속을 추가할 수 있다. 이후에 접수자는 재식별을 시도할 경우에 민형사상 처벌을 받을 수 있다. 따라서 제안된 입법안에 따르면, 비식별화된 개인정보가 계속 그러한 상태로 남아있게 되리라는 신뢰가 더해

질 것이다. Gellman의 지적에 따르면, '왜냐하면 언제라도 정보를 재식별할 수 있는지를 알 수 없으며, 사실 상 명시적으로 식별 가능한 모든 개인정보를 제외하고는 모두 PI가 되기 때문이다.'

6 구조화된 정보의 비식별화, 재식별 접근법

구조화된 정보를 비식별화하기 위한 대부분의 접근법은 정보 집합에서 특정한 식별 정보 요소를 지정하고 제거하려 한다. 이 절에서는 그러한 접근법에 사용하는 용어를 소개하고 HIPAA 프라이버시 규칙에 있는 두 가지 비식별화 기준을 논의하며, 이러한 기법에 대한 비판과 학계의 문헌에 나타난 노력에 관하여 논의한다.

6.1 직접 식별자 제거

많은 비식별화 접근법은 각각의 열에 다른 개인의 개인정보가 담긴 단일한 정보 표가 있는 정보 집합에 적용했을 때 가장 쉽게 이해할 수 있다. <표 1>에는 가상적인 정보 집합이 제시되어 있다.

직접 식별 변수(directly identifying variable) 및 직접 식별 정보(direct identifying data) 라고도 부르는 직접 식별자(direct identifier)는 "개인을 직접적으로 식별하는 정보이다." 직접 식별자의 예에는 성명, 사회보장번호, 이메일 주소 등이 있다.

ISO/TS 25237에서는 직접 식별자를 "추가적인 정보 없이, 또는 공개 영역에 있는 다른 정보를 통해 교차 연결함으로써 사람을 식별하는데 사용할 수 있는 정보"라고 정의하고 있다. 그러나 정보를 신원과 연결하기 위해서는 비록 추가적인 정보가 필요하기는 하지만, 의료보험번호와 전화번호와 같은 개인적인 다른 정보를 직접 식별자로 간주하는 것이 좋다. 왜냐하면 이러한 형태의 식별은 광범위하게 사용되고 있으며, 따라서 신원과 연결하는데 사용할 수 있기 때문이다.
HIPAA 프라이버시 규칙은 직접 식별자의 정의를 확대하여, 성명, 전화번호, 이메일 주소, 기타 고유 식별번호, 특징 또는 코드 등의 특정한 개인정보를 포괄하고 있다. 전체 목록은 6.5절에 제시되어 있다.

비식별화 중에 직접 식별자는 제거하거나 달리 변환해야 한다. 다음과 같은 접근법이 있다.

- 직접 식별자를 제거할 수 있다.
- 직접 식별자를 명백히 일반적인 범주 명칭이나 정보로 대체할 수 있다. 예를 들면, 성명은 '성명', 주소는 '거리 명 123호, 타운 명, 미국' 등으로 대체할 수 있다.
- 직접 식별자를 '*****' 또는 'XXXXX'와 같은 기호로 대체할 수 있다.
- 직접 식별자는 임의 값으로 대체할 수 있다. 만약 같은 신원이 두 번 등장하면, 두 개의 다른 값을 받는다. 이렇게 하여 원본 개인정보의 형태를 보존하고 일종의 시험

을 할 수 있게 되지만, 개인정보와 개인을 다시 연계시키기는 더 어려워진다.
- 직접 식별자를 체계적으로 가명과 대체하여 동일한 개인을 참조하는 개인기록부들이 매칭되도록 한다. 가명화(pseudonymization)에 관해서는 다음 절에서 논의한다.

<표 1> 직접 식별자를 나타내는 개인정보 표의 예

직접 식별자								
이름	주소	생일	우편번호	성별	몸무게	진단명	…	…

초기에는 개인정보를 비식별화할 때 직접 식별자를 제거하는 것에 그쳤다. 그러한 노력의 결과로 나타나는 정보는 연결 공격(linkage attack)을 통해 재식별할 수 있다. 이에 대해서는 아래의 6.3절에서 논의한다.

6.2 가명화

가명화는 성명과 개인을 직접 식별하는 다른 정보를 가명으로 대체하는 특정한 변환의 일종이다. 직접 식별자들을 모두 체계적으로 가명처리하면, 가명처리를 통해 복수의 개인정보 기록부나 정보 시스템에 걸쳐, 개인에 속하는 정보를 연결할 수 있게 된다.
만약 가명처리를 수행한 기관이 원래의 신원을 가명과 연결하는 표를 보유하고 있거나, 만약 변수를 알거나 발견할 수 있는 알고리즘을 이용하여 대체한 경우에는 가명처리를 손쉽게 되돌릴 수 있다.
가명화는 미래의 한 시점에서 가명을 되돌려 정보주체를 재식별할 수 있도록 하는 경우가 많다. 만약 직접 식별자와 가명 간의 참조(mapping)가 보존되었거나 이를 재생할 수 있는 경우에는 가명처리된 정보 집합을 되돌릴 수 있다. 예를 들어, 비밀 키를 이용하여 식별자를 암호화하여 가명을 생성할 수 있다. 키의 암호를 풀면 가명처리 과정이 역으로 되돌려지며, 원본 식별자가 생성된다. HIPAA에 따라 직접 식별자를 정보주체의 신원으로 되돌리는 작업은 포괄 기관(covered entity)라고 부르는 HIPAA의 규정에서 다루는 기관(대체로 의료 제공자)만 수행할 수 있다.

미 보건부 산하 임상연구안전국(HHS Office for Human Research Protection, OHRP)은 만약 가명처리를 쉽게 역으로 되돌릴 수 있다면, 해당 개인정보는 '코드화(coded)'된 것으로 간주되며, 생명윤리규정(Common Rule)에 따라 익명처리된 것으로 간주되지 않는다. 이러한 지침은 HIPAA의 포괄 기관 이외의 정보 집합을 이용하여 수행할 수 있으며 연방정부가 자금을 지원하는 연구에 적용된다. 그러나 만약 코드 키를 공유하는 것을 금지하는 데이터 이용 합의서가 존재한다면, 해당 정보는 식별 가능한 개인정보로 간주되지 않는다.
만약 재식별을 금지하는 데이터 이용 합의서가 없이, 가명처리된 정보 집합이 공개되면,

접수자는 가명을 되돌리거나 식별 정보를 이용하여 재식별을 시도할 수 있다. 예를 들면, 2014년 뉴욕 시 택시 리무진 위원회는 2013년에 뉴욕 시에서 탄 1억7천3백만 회의 택시 탑승 정보 집합을 공개하였다. 정보 집합을 비식별화하기 위해 이 위원회는 택시 번호와 운전사 면허번호를 단방향 암호적 해시(one-way cryptographic hash)로 대체하였다. 이 정보 집합의 이용자는 해시 알고리즘을 발견하였고, 모든 가능한 택시 번호와 면허번호를 반복적으로 적용하고 각각의 암호적 해시를 결정하며, 이 해시를 원래의 숫자로 대체함으로써 가명처리를 되돌릴 수 있었다. 따라서 비식별화 시도는 실제로 운전사의 신원을 보호하지 못했다. 이는 폭력적 공격(brute force attack)으로 알려져 있다.

가명을 되돌릴 수 있는 능력은 가명이 임의로 생성되었는가 또는 알고리즘에 의해 생성되었는가(알고리즘에 임의 키가 적용된 경우), 키의 가용성, 가명에 특이성이 있는가(unique) 아니면 재사용되었는가 등의 많은 요소에 따라 달라진다. 임의적으로 생성된 가명은 참조(mapping)가 유지된 경우에만 되돌릴 수 있다. HIPAA 프라이버시 규칙에서는 코드화 식별자인 가명을 공개하는 것을 허용하고 있다. 왜냐하면 가명은 개인에 연계된 정보에서 도출된 것이 아니기 때문이다.

비록 참조가 유지되지 않더라도, 복수의 정보 집합에 걸쳐 일관된 가명을 이용하면 연결 공격을 통해 개인정보를 재식별하기 더 쉬워질 수 있다. 이러한 이유로 인해, 제29조 개인정보 보호 작업 그룹(유럽 위원회(the European Commission)의 작업 그룹)에는 '가명처리된 개인정보는 익명처리된 정보와 동일시할 수 없다. 왜냐하면 가명처리된 개인정보는 개별 정보주체를 식별해 내고 다양한 정보 집합에 걸쳐 연결할 수 있도록 하기 때문이다'라고 언급되어 있다. 그러나 가명처리를 통해 정보와 원래의 신원을 연결할 가능성이 낮아지기 때문에, 의견(opinion)에서는 가명처리를 여전히 '유용한 보안 수단'이라고 언급하고 있다.

오랜 기간 동안 사용한 독특한 가명은 점점 더 많은 정보와 연결되기 때문에 프라이버시 위험이 증가할 수 있다. 이와 유사하게, 오래 사용한 기기 가명(device pseudonym)도 비슷한 프라이버시 위험을 야기할 수 있다. 특히 다수의 사람들에게 역동적으로 재지정된 가명과 비교할 때 그러하다.

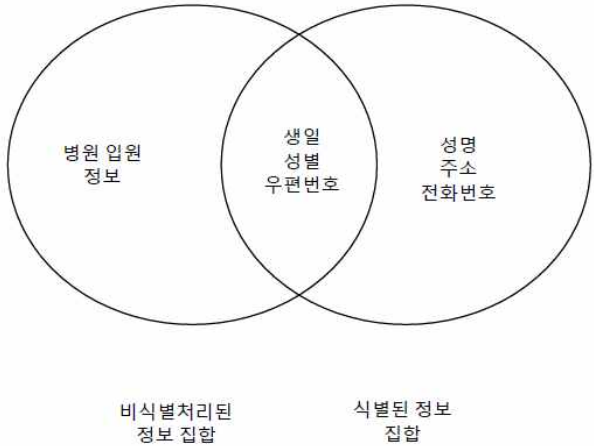
6.3 연결공격을 통한 재식별

비식별화된 정보 집합을 재식별할 수 있는 방법에는 연결 공격도 있다. 연결 공격에서는 비식별화된 정보 집합에 있는 각각의 개인기록부가, 연결 정보와 정보주체의 신원을 모두 담고 있는 두 번째 정보 집합에 있는 유사한 개인기록부와 연결된다.

가장 널리 알려진 연결 공격의 예로는 Latanya Sweeney의 공격을 들 수 있다. Sweeney는 1990년대에 자신의 MIT 졸업 과제의 일부로, 메사추세츠 주지사인 William Weld의 의료 개인기록부를 재식별하였다. 당시에 메사추세츠 주는 입원한 적이 있는 메사추세츠 주 공무원의 비식별화된 의료보험 환급 기록을 담고 있는 연구 정보 집합을 배포하고 있었다. 공무원의 프라이버시를 보호하기 위해, 정보 집합에서 성명이 제거되었으나, 공무원의 생일, 우편번호, 성별은 통계 분석을 위해 보존되었다.

Weld가 최근에 메사추세츠 병원에서 치료받은 적이 있음을 알고 있는 Sweeney는 주지사의 생일, 우편번호, 성별에 매칭되는 '비식별화된' 개인기록부를 검색하여 주지사의 개인기록부를 재식별할 수 있었다. 그녀는 이 정보를 자신이 20달러에 구입한 케임브리지 투표자 등록명부에서 얻었다. 더 나아가 Sweeney는 그녀의 발견결과를 일반화하여, 1990년 인구조사를 기초로, 미국인의 최대 87%을 다섯자리 우편번호, 생일, 성별을 이용하여 특이성이 있게(uniquely) 식별할 수 있다고 주장하였다. 프라이버시 연구자인 Phillip Golle은 후속 연구에서 2000년 인구조사를 이용하여 62%라는 재식별 비율을 계산하였다. 컬럼비아 대학교의 Daniel C. Barth-Jones 교수는 이 연구를 비판하며, 1996~1997년 사이에 케임브리지 시 인구의 55%만 등록하였으며, 따라서 투표자 명부와 연계시켜 케임브리지 시 인구의 55% 이하만을 재식별할 수 있었다고 지적하였다.

Sweeney의 연결 공격은 다음과 같이 그림으로 나타낼 수 있다.



(그림 3) 연결 공격은 두 개 이상의 정보 집합의 정보를 조합하여 개인기록부를 재식별

많은 요소들이 그러한 연결 공격을 복잡하게 만든다.

- 연결하기 위해서는 한 사람이 두 정보 집합에 모두 있어야 한다. Sweeney는 Weld가 입원한 적이 있고, 주지사로서 등록된 투표자임을 알고 있었기 때문에 두 정보 집합에 모두 있다는 것을 알았다.
- 두 정보 집합에 모두 있는 변수를 연결함으로써 특이성이 있고 분간되는 개인기록부만 특이성이 있게(uniquely) 연결할 수 있다. 그렇지 않을 경우에는 연결에 확률론적 관점을 취해야 한다(예, 만약 두 가지 가능한 매칭이 있다면 정확하게 매칭될 확률은 0.5이다). 특이성이 있게 매칭되는 경우에는 한 개인의 개인기록부는 만약 같은 생일, 성별, 우편번호를 가진 사람이 두 정보 집합에 없어야만 연결할 수 있다. 결과에 나타난 바와 같이, 케임브리지 시의 투표자 명부에 등록된 사람 중에 Weld와 생일이 같은 사람은 없었다. 그러나 만약 Weld의 개인기록부를 현재의 HIPAA 기준에 따라 비식별화하였다면 개인기록부에는 그의 출생연도와 우편번호의 앞 세 자리만 포함되

어 있었을 것이다. 이러한 조건에서는 특이성이 있는(unique) 매칭은 아마도 불가능했을 것이다.

- 두 정보 집합에서 변수가 같지 않다면 연결하기 위해서는 해당 정보를 정규화하거나 달리 일관되도록 해야 한다. 이러한 정규화(normalization) 과정에 오류가 발생할 수 있다. 이는 Weld의 사례에서는 문제가 되지 않았지만, 만약 한 정보 집합이 '연령'을 보고하고 다른 정보 집합이 '생일'을 보고했다면 문제가 될 수 있다.
- 어떤 사람은 정보 집합에 특이성이 있게 나타나지만, 집단에서는 특이성이 없을 수 있다. 즉, Weld와 생일이 같은 다른 사람이 케임브리지 시에 있었을 수 있지만 그 사람이 투표에 등록하지 않았다면 분석에서 그 사람을 누락했을 것이다.
- 어떤 연결이 정확한지를 검증하기 위해서는 연결 작업의 일부로 사용하지 않은 정보를 이용해야 한다. 이 경우, Weld의 의료 개인기록부는 Weld의 입원에 관한 신문기사를 이용하여 검증할 수 있었다.

데이터 이용 합의서와 사용자 클릭 라이선스 합의서를 통해 관리 측면에서 재식별을 금지할 수 있다. 그러나 이러한 합의서는 자유롭게 공개된(예를 들면 인터넷에 공개) 비식별화 정보 집합에는 적용하기 어려울 수 있다

6.4 준-식별자의 비식별화

간접 식별자(indirect identifier) 또는 간접 식별변수(indirectly identifying variable)라고도 부르는 준-식별자(quasi-identifier)는 자체로서는 특정한 개인을 식별하지 않지만 다른 정보와 조합하거나 '연결'하여 정보주체를 식별할 수 있다. Sweeney는 William Weld의 의료 개인기록부를 재식별할 수 있었는데, 이는 생일, 우편번호, 성별이 준-식별자이기 때문이다.

<표 2> 직접 식별자와 준-식별자를 보여주는 개인정보 표의 예

직접 식별자		준-식별자						
이름	주소	생일	우편번호	성별	몸무게	진단명	…	…

준-식별자는 비식별화에 중대한 문제를 야기한다. 직접 식별자는 정보 집합에서 제거할 수 있는데 비해, 준-식별자는 일반적으로 나중의 분석에서 중요할 수 있는 정보를 담고 있으며, 준-식별자를 제거하면 정보 집합의 효용성이 줄어들 수 있다. 그렇기 때문에 재식별 위험과 준-식별자를 포함하여 얻는 유용성 간에 균형을 잡기 위한 세심한 고려가 필요하다.

준-식별자를 비식별화하기 위해 몇 가지 방법을 이용한다.

1) 범주화(suppression) : 준-식별자를 범주화하거나 제거할 수 있다. 정보를 제거하면 프라이버시 보호가 극대화되지만 정보 집합의 효용이 감소할 수 있다.
2) 일반화(generalization) : 특정한 준-식별자 값이 주어진 범위 안에 있다고 보고하거나 어떤 세트의 한 요소로서 보고할 수 있다. 예를 들면, 우편번호 12345를 12000과 12999사이의 우편번호로 일반화할 수 있다. 일반화는 예를 들면 극단치(outlier)를 식별하여, 전체 정보 집합 또는 특정한 개인기록부에 적용할 수 있다.
3) 인자변환(perturbation) : 규정된 일반화 수준 이내에서, 각 개인에 대해 일관된 방식으로 특정한 값을 다른 값으로 교체할 수 있다. 예를 들면, 모든 연령을 원래 연령의 (-2 … 2)년으로 임의로 조정하거나 또는 입원 또는 퇴원 일자를 체계적으로 같은 일자로 (-1000 … 1000)일을 이동시킬 수 있다.
4) 교환(swapping) : 규정된 일반화 수준 이내에서 개인기록부 간에 준-식별자 값을 교환할 수 있다. 교환은 통계적 특징을 유지할 필요가 있을 경우에는 주의하여 다루어야 한다.
5) 하위 샘플링(sub-sampling) : 비식별화를 수행하는 기관은 전체 정보 집합을 공개하는 대신에 샘플을 공개할 수 있다. 만약 하위 샘플만을 공개한다면 재식별 가능성은 낮아진다.

k-익명성은 주어진 프라이버시 수준을 달성하기 위해 준-식별자에 필요한 조작 횟수를 정량화하기 위해 Sweeney가 개발한 기법이다. 이 기법은 모든 준-식별자 값에 매칭되는 개인기록부 세트인 동질집합(equivalence class)이라는 개념을 기반으로 하고 있다. 준-식별자로 이루어진 모든 조합에 대해 최소한 k개의 매칭되는 개인기록부가 있는 경우, 해당 정보 집합은 k-익명성이라고 말한다. 예를 들면, 만약 준-식별자인 출생연도와 주(state)가 있는 정보 집합이 k=4 익명성이 있다면, 모든 (출생연도, 주) 조합에 대해 최소한 4개의 개인기록부가 있다. 이후의 연구를 통해 각각의 동질집합 내의 민감한 속성의 다양성(l-다양성)에 대한 요건을 추가하고, 결과 정보가 원본 정보에 통계적으로 근접할 것을 요구하여(t-근접성) k-익명성을 정교화하였다.

Khaled El Emam 교수와 Bradley Malin 교수는 식별자와 준-식별자를 분류하여 11단계로 된 개인정보의 비식별화를 위한 과정을 개발하였다.

- 1단계 : 정보 집합에서 직접 식별자 결정 : 전문가가 정보 집합에서 정보주체를 식별하는 데만 사용하는 요소를 결정한다.
- 2단계 : 직접 식별자 마스킹(변환) : 직접 식별자를 제거하거나 가명으로 대체한다.
- 3단계 : 위협 모델화 : 기관은 '가상의 적', 그들이 재식별을 위해 사용할 수 있는 추가적인 정보, 적들이 재식별을 위해 사용할 수 있는 준-식별자를 결정한다.
- 4단계 : 최소 허용 정보 효용을 결정 : 이 단계에서 기관은 각각의 항목에 대해 일어

날 수 있는 최대의 비식별화의 양을 결정하기 위해 비식별화된 개인정보가 이용될 수 있는 용도를 결정한다.

- 5단계 : 재식별 위험의 한계치 결정 : 기관은 선례와 기준(예, 작업 문서 22 : 통계적 공개 통제에 관한 보고서)을 이용하여 정보에 대한 작업과 통제 완화 가능성에 관련된 허용 가능한 위험을 결정한다.
- 6단계 : 데이터베이스에서 (샘플) 정보를 가져옴(import) : (식별된) 소스 데이터베이스에서 정보를 획득하기 위한 노력이 클 수 있기 때문에, 연구자들은 계획에 도움을 주기 위해 시험적인 정보 수입을 권고한다.
- 7단계 : 실제 재식별 위험을 평가 : 실제의 식별화 위험을 계산한다.
- 8단계 : 실제 위험을 한계치와 비교 : 5단계와 7단계의 결과를 비교한다.
- 9단계 : 변수를 설정하고 정보 변환을 적용 : 실제 위험이 허용 가능한 수준이라면, 비식별화 변수를 적용하고 정보를 변환한다. 위험이 너무 큰 경우, 새로운 변수 또는 변환을 고려해야 한다.
- 10단계 : 해법에 대한 진단 수행 : 비식별화된 개인정보가 충분한 효용성을 갖고 있으며, 허용 가능한 변수 이내에서 재식별이 불가능하도록 하기 위해, 비식별화된 개인정보를 분석한다.
- 11단계 : 변환된 정보를 외부 정보 집합으로 내보냄(export). 마지막으로, 비식별화된 개인정보를 수출하고, 비식별화 기법을 서면 보고서에 기록한다.

직접 식별자와 준-식별자를 기초로 한 비식별화에 대한 주된 비판은 준-식별자를 관리적으로 결정할 때에는, 비식별화를 수행할 당시에 없었지만 나중에 존재하게 된 정보 등의 외부 정보와 조합되거나 연결되었을 때 특이성이 있게 식별하는 변수를 누락할 수 있다는 점이다.

현실적인 입장을 취하고 발생 가능성이 높은 공격을 고려하는 것이 중요하다. 재식별, 다른 정보와의 연결, 미인가 공유를 금지하는 데이터 이용 합의서가 있는 경우에는 특히 그러하다. 식별자의 선정에 대한 지침이 되는 기준 및 허용 가능한 위험 수준에 관한 선례 이외에도, 평가 또는 재식별 위험은 적이 현실적으로 알 수 있는 정보의 양('공격자의 힘')으로 한정될 수 있다.

6.5 HIPAA에 따른 개인의료정보(Protected Health Information, PHI)의 비식별화

1996년 HIPAA 프라이버시 규칙에는 개인의료정보(PHI)의 비식별화에 관하여, 전문가 활용법(Expert Determination Method, §164.514(b)(1))과 세이프 하버 방식(the Safe Harbor method, §164.514(b)(2)) 등 두 가지 접근법이 제시되어 있다. 두 방식 모두 재식별 위험이 전혀 없는 안전한(foolproof) 비식별화 방식은 아니다. 단, 이 방법들은 재식별 위험을 낮추면서 비식별화된 의료 정보를 생산하고 공유할 수 있도록 하기 위한 실용적인 접근법을 취하고 있다.

6.5.1 HIPAA 전문가 활용법

'전문가 활용법(the Expert Determination method)'은 개인의료정보를 검토하는 전문가를 제공하며, 재식별 위험을 최소화하는 적절한 비식별화 수단을 정한다. 프라이버시 규칙에는 다음과 같은 특별한 조항이 있다.

"(1) 개별적으로 식별할 수 없는 정보의 제작에 관해 일반적으로 인정되는 통계학 및 과학적 원리와 방법에 관한 적절한 지식과 경험을 갖춘 사람

(i) 그러한 원칙과 방법을 적용하여, 예상되는 정보 접수자가 그러한 정보를 이용하거나 또는 합리적으로 이용할 수 있는 다른 정보를 이용하여, 정보주체인 개인을 식별하기 위해 해당 정보를 이용할 수 있는 위험이 매우 적다고 결정한다.

(ii) 그러한 결정을 뒷받침하는 방법과 분석 결과를 문서로 기록한다."

6.4절에 제시된 El Emam과 Malin 방법론은 전문가 활용법의 예라고 할 수 있다.

본 절과는 별도로, 프라이버시 규칙이나 미국 보건복지부(the Department of Health and Human Services, HHS) 시민권실(Office of Civil Rights)은 전문가에 관한 기준이나 자격을 명시하고 있지 않으며, 전문가를 이용하는 기관의 공개 요건이나 심지어 전문가의 결정이 내려졌는지를 인정하기 위한 요건도 명시하고 있지 않다. 또한 재식별 위험의 계산 또는 정량화 방법도 명시되어 있지 않으며, 허용 가능한 최소한의 재식별 위험이 '매우 적어야' 한다는 점 외에는 다른 규정이 없다.

전문가 활용법에는 전문가가 "일반적으로 인정되는 통계적, 과학적 원리와 방법"을 알고 적용해야 한다고 명시하고 있으며, 이는 통계적 공개 통제와 비식별화 방법에 관한 문헌을 알고 있어야 함을 의미할 것이다. 비식별화와 위험 수준에 관한 강력한 선례도 존재하고 있으며, 효과적인 비식별화 방법론에 적용되어야 한다.

6.5.2 HIPAA 세이프 하버 방식

'세이프 하버(Safe Harbor)' 방식은 포괄 기관이 '개인, 친척, 직원 또는 개인의 가족'에 관한 18가지 특정 유형의 개인정보를 삭제함으로써 개인정보를 비식별화된 것으로 다루도록 한다. 18가지 유형은 다음과 같다.

"(A) 성명

(B) 주(state) 이하의 모든 지리적 행정구역으로서, 거리 주소(street address), 시(city), 카운티(county), 지구(precinct), 우편번호(Zip code) 및 그와 동등한 지오코드(geocode)를 포함하나, 미국 통계국이 현재 공개한 우편번호의 앞 세 자리는 제외한다.

(1) 앞자리 세 개가 동일한 모든 우편번호를 조합하여 형성된 지리적 단위에는 20,000명 이상이 포함된다.

(2) 20,000명 내외의 사람이 포함된 그러한 모든 지리적 단위의 우편번호 앞 세 자리를 000으로 변경한다.

(C) 생일, 입원일, 퇴원일, 사망일, 89세 이하의 모든 연령 등, 개인과 직접적으로 관련

된 모든 날짜의 모든 날짜 요소(년은 제외) 및 그러한 연령을 나타내는 날짜의 모든 요소(년 포함), 단, 단일한 90세 이상의 범주로 종합할 수 있는 연령 및 요소는 제외한다.

(D) 전화 번호
(E) 팩스 번호
(F) 이메일 주소
(G) 사회보장번호
(H) 의료기록번호
(I) 의료보험(Health Plan) 수혜자 번호
(J) 계좌번호
(K) 자격증/면허 번호
(L) 차량 식별자 및 일련번호, 차량 번호판 번호 포함
(M) 기기 식별자 및 일련번호
(N) 웹 URL(Universal Resource Locator)
(O) 인터넷 프로토콜(IP) 주소
(P) 지문이나 성문(voiceprint)을 포함한 바이오인식인증 식별자
(Q) 얼굴 전체의 사진 및 그와 유사한 이미지
(R) 기타 특이한(unique) 식별 번호, 특징 또는 코드

세이프 하버 방식은 전문가 활용법에 비해 규칙을 직접적으로 적용할 수 있고 과정을 반복할 수 있으며, 합법적으로 비식별화된 정보 집합을 제공한다.

어떠한 방법을 사용하더라도, 비식별화를 수행하는 포괄 기관은 “정보를 단독으로 사용하거나, 다른 정보와 함께 사용하여 정보주체인 개인을 식별할 수 있다는 실제적인 지식을 갖고 있지” 않아야 한다. 그럼에도 불구하고 HHS는 단순히 재식별 기법의 존재를 알고 있는 것은 ‘실제적인 지식’ 기준에 부합되지 않는다는 특별 지침을 내렸다.

Q: ‘3.7: 만약 포괄 기관이 보건 정보를 재식별하는 방법에 관한 특정한 연구를 알고 있거나 비식별화된 보건 정보를 단독으로 또는 다른 정보와 조합하여 사용함으로써 개인을 식별할 경우, 이는 필연적으로 해당 포괄 기관이 세이프 하버 방식에 따른 실제적인 지식을 갖고 있음을 의미하는가?

A: ‘아니다. 특정한 분석 능력과 정량화 능력을 가진 연구자들이 정보를 특정한 방식으로 조합하여 건강 정보를 식별하는 능력에 관한 많은 문헌이 있다. 포괄 기관은 나머지 정보를 식별하기 위한 방법에 관한 연구나 비식별화된 정보를 단독으로 또는 다른 정보와 조합하여 사용함으로써 개인을 식별하는 연구에 관하여 알고 있을 수 있다.

그러나 그러한 연구와 방법에 대한 포괄 기관의 단순한 지식은 그 자체로서는 그러한 기관이 공개하는 개인정보에 그러한 방법이 이용될 것이라는 ‘실제적인 지식’을 갖고 있음을 의미하지 않는다. OCR은 비식별화된 개인정보를 받는 모든 잠재적인 접수자들이 그러한 능력을 갖고 있다고 포괄 기관이 간주할 것이라고 예상하지 않는다. 이는 어떤 정보가 적절히 비식별화되었는지 결정하기 위한 단순한 방법을 포괄 기관에게 제공하려는 세이프 하버 방식의 의도에 부합되지 않을 것이다.

6.5.3 HIPAA 세이프 하버 방식의 효과 평가

HIPAA 세이프 하버 방식은 Sweeney의 연구에 많은 영향을 받았다. 세이프 하버 방식은 Sweeney의 연구를 언급하고 있고, 그녀가 일반화를 위해 식별한 준-식별자에 특히 주목하고 있다(우편번호와 생일). 예를 들면, 우편번호 첫 세 자리와 출생연도에 대한 보고를 허용하는 등, 이 방법은 재식별 위험과 정보 집합의 효용성의 유지 사이에 균형을 이루려는 것으로 보인다.

의료 개인기록부의 비식별화와 비식별화된 개인정보의 재식별 위험의 측면에서 HIPAA 세이프 하버 방식의 효과에 관한 논란이 있다. Sweeney는 미국 전역의 특이성이 있는 재식별 위험을 0.04%로 예측하였는데, 이는 10,000개의 개인기록부 가운데 4개를 특이성이 있게 재식별할 수 있음을 의미한다. 반더빌트 건강 정보 프라이버시 연구소(Vanderbilt Health Information Privacy Lab)의 Kathleen Benitez와 Bradley Malin은 주(state)별로 연구를 수행하여 특이성이 있는 재식별 위험은 0.01%와 0.25% 사이라고 결론지었다. 그러나 이는 특이성이 있는 식별정보가 출생연도, 성별, 3자리 우편번호인 개인정보로 한정된다. Sweeney는 워싱턴 주가 판매한 건강 개인정보를 공격할 때, 세이프 하버 방식에 언급된 준-식별자를 제외한 다른 준-식별자로 인한 위험도 있음을 확인하였다.

미국 보건복지부의 국가의료정보기술 조정관실(Office of the National Coordinator for Health Information Technology, ONC HIT)은 2010년에 HIPAA 세이프 하버 방식에 대한 검사를 수행하였다. 이 연구의 일환으로, 의료 시스템에서 나온 2004~2009년 간 히스패닉계 시민의 병원 입원 개인기록부 15,000건을 연구자들에게 제공하였다. 연구자들은 비식별화된 개인기록부와 미국인 2억3천5백만 명의 정보를 갖고 있다고 주장하는 회사인 InfoUSA에서 구입한 30,000건의 개인기록부의 매칭을 시도하였다. 미국 인구조사 자료에 근거하여, 연구자들은 판매된 개인기록부 30,000건이 대략 병원 환자 5,000명을 포괄하고 있다고 추정하였다. 실험자들이 성별, Zip3(HIPAA에 따라 허용된 대로, 우편번호의 앞 세 자리), 연령을 이용하여 매칭했을 때, 병원 자료에서 216건의 특이성이 있는 개인기록부를 발견하였고, InfoUSA의 자료에서 84건의 특이성이 있는 개인기록부를 발견하였으며, 두 자료에서 모두 매칭된 개인기록부는 20건이었다. 이어서 연구자들은 이 20건의 매치를 검토하여 20개 중 2개만 같은 성(姓), 거리 주소, 전화번호를 갖고 있음을 확인하였다. 이는 특이성이 있는 재식별 비율이 0.013%임을 나타낸다. 또한 연구자들은 더 보수적인 방법을 이용하여 특이성이 있는 재식별 위험을 0.22%로 계산하였다. 이러한 비율들은 단일한 의료보험 시스템에 속한 단일한 민족 집단을 이용한 것이기 때문에 국가 전체 평균이 아니다.

6.5.4 HIPAA 제한된 정보 집합

개인의료정보를 담고 있는 정보와 비식별화된 개인정보에 추가하여, HIPAA 프라이버시 규칙은 제한된 정보 집합(limited dataset)이라는 세 번째 유형의 정보를 인정하고 있다. 프라이버시 규칙에 따르면, 제한된 정보 집합은 부분적으로 비식별화되었지만, 여전히 날

짜, 시, 주, 우편번호, 연령을 포함하고 있는 정보 집합이다. 그러한 정보는 개인의료정보로 간주되지만, 해당 개인정보를 공유하는 기관이 데이터 이용 합의서를 집행할 경우, 연구, 공중 보건, 의료보험 운영을 위해 공유할 수 있다. 최저 기준으로서, 데이터 이용 합의서는 보안 안전조치(safeguards)를 요구하고 해당 개인정보를 이용하는 모든 사람이 유사한 제한을 받을 것을 요구하며, 재식별 및 다른 정보와의 무단 연결, 정보주체와의 접촉을 금지해야 한다.

Benitez와 Malin은 제한된 정보 집합의 재식별 위험이 10~60%인 것으로 확인함으로써, 제한된 정보 집합은 적절히 비식별화된 것으로 간주하지 말아야 한다는 점을 다시 한 번 보여주고 있다.

6.6 비식별화에 대한 평가

비식별화에서 정보 집합의 일부 개인정보란에 식별될 가능성이 없는 유용한 정보가 들어있다는 것을 가정한다.

최근 몇 년에 발표된 많은 학술 연구에서는 많은 개인정보 항목이 식별정보일 수 있으며, 정보주체의 신원이 있는 적절한 정보에 대한 접근권(access)이 있고, 재식별이나 연결에 관한 금지가 없는 고차원 정보에서 개인을 식별할 수 있는 경우가 많다는 사실을 보여주었다.

- 넷플릭스 상(the Netflix Prize) : 2008년에 Narayanan과 Shmatikov는 사람들이 본 영화를 식별자로 이용할 수 있는 경우가 많다는 점을 보여주었다. 넷플릭스는 일부 고객이 관람한 영화로 된 정보 집합을 공개하였고, 자사의 넷플릭스 상 경연의 일부로서 순위를 매겼다. 비록 정보 집합에는 직접 식별자가 없었지만, 연구자들은 관람한 영화 세트(특히 인기가 적은 컬트 고전과 외국 영화)를 이용하여, 넷플릭스 정보 집합의 사용자 프로필과 비식별화가 되지 않았고, 실명이 많이 포함된 사용자 성명이 있는 인터넷영화 데이터베이스(the Internet Movie Data Base, IMDB)에 있는 단일한 사용자 프로필을 매칭시킬 수 있는 경우가 많다는 점을 보여주었다. 위협 시나리오에 따르면, 사람들의 IMDB 프로필을 넷플릭스 상 정보와 연결할 수 있기 때문에, IMDB에 몇 가지 영화의 순위를 매김으로써, 의도치 않게 자신이 관람한 모든 영화를 공개할 수 있다는 것이다.
- 의료 검사 : 2013년에 Atreya 등은 환자의 실험 결과 5~7개를 “비식별화된 생물의학 연구 데이터베이스에 있는 상응하는 개인기록부를 확인할 수 있는 검색 키”로 활용할 수 있다는 점을 보여주었다. 환자 61,280명의 비식별화된 검사 결과 850만 건으로 된 반더빌트 대학의 정보 집합을 이용하여, 연구자들은 검사에 따라, 정보 집합에 있는 연속적인 실험실 검사 결과 4개의 34%~100%를 특이성 있게 분간할 수 있다는 점을 발견하였다. 가장 흔한 검사 결과인 CHEM7과 CBC는 각각 검사 주체의 98.9%와 98.8%를 분간하였다. 위협 시나리오에 따르면, CHEM7 또는 CBC 검사 결과를 담고 있는 단일한 실험실이 식별한 보고서를 중간에서 가로채는 경우(아마도 쓰레기통 같은 곳에서), 이를 이용하여 해당 개인에 속하는 다른 개인기록부를 비식별화된 생물의료 연구 데이터베이스에서 검색할 수 있다.

- 신용카드 거래 : Montjoye 등은 무명의 국가에서 나온 샘플 110만 명의 비식별화된 신용카드 거래 수집자료에서, 네 개의 구분되는 공간 및 시간적 지점을 이용하면 샘플 안의 개인의 90%를 특이성 있게 식별하는데 충분하다는 점을 보여주었다. 지리적 정밀도를 낮추고 거래액을 버리면(예, 구매액 14.86달러를 10.00달러와 19.99달러 사이로 보고함), 필요한 지점의 수가 늘었다.
- 이동 궤적 : Montjoye 등은 사람과 차량을 ‘이동 궤적(mobility traces)’(사람이나 차량이 방문한 장소와 시간 기록)을 이용하여 식별할 수 있다는 점을 보여주었다. 그들은 연구에서 150만 명으로 이루어진 샘플의 궤적 정보를 처리하였고, 시간 값은 시(hour)로 일반화하고, 공간 정보는 핸드폰 시스템이 제공한 해상도로 일반화하였다(통상적으로 10~20개 도시 블록). 연구자들은 특정한 장소와 시각에 매칭시킨 개인에 대한 임의로 선정한 관찰결과 4개를 이용하여 정보주체의 95%를 특이성 있게 식별할 수 있다는 점을 발견하였다. 개인의 위치/시간 지점은 신용카드 구매, 사진, 인터넷 등 다양한 출처에서 수집할 수 있다. Ma 등이 수행한 유사한 연구에 따르면, 10개의 주변적 정보를 이용하여 개인을 30~50% 식별할 수 있음을 보여주었다. 위협 시나리오에 따르면, 공격자는 공개된 정보 집합에서 장소/시간 쌍 5개를 노출한 개인(예를 들면, 1개월 동안 집과 직장에서 이메일을 4번 발송)의 전체 이동 궤적을 식별할 수 있을 것이다. 위와 마찬가지로, 공격자는 목표물이 정보 안에 있었음을 알아야 할 것이다.
- 택시 승차 정보 : 2014년 뉴욕 시 택시 리무진 위원회는 2013년의 모든 뉴욕 시 택시 승차 기록(총 1억7천3백만 건)이 담긴 정보 집합을 공개하였다. 이 정보에는 택시 기사나 탑승자의 성명이 포함되어 있지 않았지만, 택시의 번호판 번호로 쉽게 변환할 수 있는 32자리로 된 알파벳숫자 코드가 포함되어 있었다. Neustar사의 한 인턴 정보 과학자는 택시 번호판을 분명히 볼 수 있는 택시에 타고 내리는 유명인사가 담긴 시간이 찍혀 있는 사진을 인터넷에서 찾아낼 수 있음을 알게 되었다. 그 인턴은 이 정보를 이용하여 1억7천3백만 건의 택시 승차 중 2건의 택시 도착지, 택시요금, 팁 등을 알 수 있었다. Gawker 웹사이트의 한 리포터는 9개를 더 식별할 수 있었다.

택시 정보에 관한 경험에 따르면, 개인정보 기록에 있는 다른 정보와 연관될 수 있는 예상치 못한 정보 출처가 많다는 점을 보여주며, 직접 식별자를 변환할 때 매우 조심해야 한다는 점을 보여주고 있다. 택시와 이동 궤적에 대한 연구에 따르면, 지리공간적 정보의 식별 능력이 매우 크다는 점을 알 수 있다. 개인의 위치와 시간에 대한 몇 가지 관찰 정보만 있다면, 비록 일반화되고 잡음이 있는 정보 집합 안의 정보라고 해도, 식별 가능성이 매우 높아질 수 있다. 또한 일부 위치는 독립된 위치이거나 사진정보가 많기 때문에 매우 식별력이 크다.

이러한 유형의 연구에 대한 비판은, 샘플 안에 있는 특이성(uniqueness)과 집단 안에 있는 특이성을 구분하지 못하는 경우가 많다는 점이다. 예를 들면, Montjoye 등의 연구에 따르면, 지리 공간적 지점 4개에서 개인을 분간할 수 있다는 연구결과는 만약 목표로 한 개인이 샘플 안에 있다는 추가적인 정보를 공격자가 갖고 있을 경우에만 적용된다. 만약 샘플 크기가 전체 집단까지 커진다면, 특이성을 식별하는데 필요한 지점의 수도 증가할 수 있다.

또한 의료 검사와 택시 연구에서는 모두 정보에 비교적 적은 인자변환(perturbation)이 있을 경우에는 재식별이 어렵거나 불가능하게 될 수 있다는 점도 보여주고 있다. Atreya 등이 검토한 의학 검사 결과에서 저자들은 임상적 중요성을 크게 변화시키지 않으면서도 식별 정보를 제거하는 방식으로 임상적 수치에 적응적 잡음(adaptive noise)을 추가하는 단순한 비식별화 알고리즘을 제시하고 있다. 택시 연구의 경우, 택시 번호판 가명을 되돌릴 수 있었기 때문에 유명인사들이 식별되었다. 만약 번호판을 적절히 보호하였거나 GPS 위치정보가 100제곱미터짜리 그리드에 종합되었더라면 재식별 위험은 상당히 줄었을 수 있었으며, 프라이버시에 대한 영향은 무시할 수 있었을 것이다.

El Emam 등은 2001년부터 2010년까지 발간된 재식별 시도 14건을 검토하였다. 저자들은 각각에 대해 의료 정보가 포함되어 있었는지, 적의 직업이 무엇인지, 재식별이 일어난 국가는 어디인지, 재식별된 개인기록부의 비율은 어떠한지, 비식별화에 적용된 기준은 무엇인지, 재식별이 검증되었는지를 확인하였다. 연구자들은 현행 기준에 따라 비식별화되지 않은 작은 정보 집합의 경우에 재식별에 성공하는 경우가 많았음을 확인하였다. 많은 경우에 재식별 연구자들은 단지 몇 개의 개인기록부만 재식별하였고, 그러한 재식별이 검증되지 않았을 수도 있었다. 그렇기 때문에, 이러한 사례에서 과학적 결론을 도출하기는 어렵다.

6.7 재식별 위험의 추정

위의 예에서 알 수 있듯이, 개인정보를 다루는 개인과 기관은 주어진 특정한 비식별화 절차의 재식별 위험을 계산하기 위해 쉽고 신뢰성 있는 절차가 필요하다. 샘플링한 정보 집합 안의 다양한 개인의 구분 가능성, 비식별화 알고리즘, 연결 정보의 가용성, 재식별 공격을 수행할 수 있는 개인의 범위 등의 여러 가지 요소에 따라 달라지기 때문에 이러한 위험의 계산은 복잡하다.

재식별 위험의 종류도 다양하고 위험의 보고 방식도 다양하다. 모델은 식별되는 주체 각각의 평균 위험을 보고할 수 있고, 어떤 주체가 식별될 수 있는 위험을 보고하거나, 어떤 주체가 다양한 k명의 개인 가운데 1인 것으로 식별될 수도 있다.

Dankar 등은 다양한 종류의 정보 출처의 구분가능성(distinctiveness)을 추정하기 위한 통계적 모델과 결정 규칙을 제안하고 있다. El Eman 등은 단일한 개인기록부를 식별하는 것이 목표인 '동기가 약한 적'과 모든 매칭을 식별하고 검증하며, 실제적 또는 금전적 제한만을 받는 '동기가 강한 적'이라는 두 가지 공격자 모델을 이용하여 약물 부작용 보고서를 재식별할 위험을 모델화하는 기법을 개발하였다. 일반적으로, 기관들은 모든 개인정보 요소(연속적 요소 및 범주적 요소)를 준-식별자로 취급하는 결정과 재식별 가능성과 공개하는 실질적으로 변경되지 않은 개인정보의 유용성 간에 균형을 잡아야 한다. 비식별화를 할 경우에는 정보 안의 통계적 관계에 심각한 손상을 입혀, 비식별화한 개인정보의 유용성이 제한될 수 있다.

7 비구조화된 개인정보의 비식별화

지금까지는 구조화된 개인정보의 비식별화를 주로 다루었지만, 본 장에서는 구조화되지 않은 문서와 멀티미디어 데이터를 비식별화하는 문제를 다룬다.

7.1 의료문서의 비식별화

의료 문서에는 구조화되지 않은 문안이 상당히 많이 포함되어 있다. 최근 몇 년 동안, 자유로운 양식의 문서(예를 들면, 서술형으로 된 섭취 보고서)에서 평서문 처리 기법을 이용하여 HIPAA 정보 요소 18개를 제거하기 위한 도구를 개발하고 평가하려는 노력이 있었다. 주로 연구한 두 가지 기법은 규칙을 기반으로 한 시스템과 통계를 기반으로 한 시스템이 있다. 규칙을 기반으로 한 시스템은 특정 유형의 문서에 잘 적용되지만, 새로운 영역에 적용했을 때에는 잘 작동하지 않는 경향이 있다. 통계적 기법은 일반적으로 규칙을 기반으로 한 시스템에 비해 정확도가 낮고 라벨링된(labeled) 훈련 정보가 필요하지만, 새로운 분야에 적용하기 쉽다는 장점이 있다.

평서문을 비식별화하는데 있어 다양한 요소들이 장애가 된다.

1) 성명과 주소 등의 직접 식별자를 분명하게 표시할 수 없을 수 있다.
2) 중요한 의료 정보를 개인정보로 착각하고 삭제할 수 있다. 의학에서 질병을 설명하는데 흔히 사용하는 사람이름이 붙은 병명의 경우에는 특히 문제가 된다(예, 애디슨병(Addison's Disease), 벨 마비(Bell Palsy), 라이터 증후군(Reiter Syndrome) 등)
3) HIPAA 세이브하버 요소 18개를 제거한 후에도 정보에서 의료 주체를 식별할 수 있을 수 있다.

몇몇 연구자들이 문서 비식별화 도구에 대한 정식 평가를 수행한 바 있다.

- 2012년에 신시네티 아동병원 의료 센터(Cincinnati Children's Hospital Medical Center, CCHMC)의 Deleger 등은 MALLET 기계학습 패키지를 기반으로 CCHMC가 자체 개발한 시스템인 MCRF에 대해 MITRE 식별 스크러버 툴킷(Identification Scrubber Toolkit, MIST)을 검사하였다. 참조 말뭉치(corpora)는 2010년에 CCHMC에서 작성한 5백만 건의 개인기록부에서 선정한 3,503건의 임상 개인기록부, 2006 i2b2 비식별화 도전 말뭉치(de-identification challenge corpus), PhysioNet 말뭉치였다.
- 2013년에 유타 대학교(the Univeristy of Utah) 생의학 정보공학과(Department of Biomedical Informatics)의 Ferrandez 등은 자동 비식별화 시스템 5개를 2개의 참조 말뭉치에 대해 평가하였다. 이 검사는 비식별화하고 합성 정보를 더한 문서 889건으로 이루어진 2006 i2b2 비식별화 도전 말뭉치와 미 보훈보건청(Veterans Health Administration, VHA)이 제공한 2008년 4월 1일과 2009년 3월 31일 사이의 단어 500개 이상인 문서에서 임의로 추출한 문서 800건으로 이루어진 말뭉치를 이용하여 수행하였다.

- 2013년에 국립 의학도서관(the National Library of Medicine, NLM)은 도서관 산하 과학 자문관 위원회(Board of Scientific Counselor)에게 '임상 문서 비식별화연구(Clinical Text De-Identification Research)'라는 제목의 보고서를 발간하였는데, 여기에서 NLM은 자체적으로 개발한 도구인 NLM Scrubber(NLM-S)와 MIT의 비식별화 시스템(MITdeid), MIST를 비교하였다. 이 검사는 1,073건의 의사관찰보고서(Physician Observation Reports)와 NIH 임상센터(Clinical Center)의 2,020건의 환자 연구 보고서로 이루어진 내부 말뭉치를 이용하여 수행하였다.

CCHMC와 유타 대학교의 연구는 모두 원 상태의 시스템을 검사하였고, 글뭉치의 일부를 훈련 정보의 일부로 사용하여 조정한 후에 검사하였다. 유타 대학교의 연구에서는 공개하기 위한 VHA의 개인기록부를 충분히 비식별화하지 못하였고, 규칙에 기반한 시스템은 특정한 유형의 정보를 잘 찾아냈지만(예, 사회보장번호, 전화번호), 다른 종류의 정보에 대해서는 훈련 가능한 시스템이 더 나은 결과를 보인다는 점을 발견하였다. 시스템에 약간의 변경이 있었지만, 모두 유사한 성능을 나타냈다. NLM의 연구에서는 NLM-S가 MIST와 MITdeid를 크게 능가하였고, NLM 정보 집합에서 HIPAA 세이프 하버 기준에 매칭되는 식별자의 99.2%를 제거하였다. 저자들은 나머지 식별자들이 환자의 프라이버시에 크게 위협이 되지 않을 것이라고 결론지었다.

Meystre, Shen 등의 연구에 의하면, 솔트레이크 시티(Salt Lake City) VHA 의료 센터의 자동적으로 비식별화된 퇴원 정보에서는 환자의 의사 또는 치료 전문가를 식별할 수 없었다. Carrell 등의 연구에서는 비식별화된 문서에서 '환자(Patient)' 및 '주소(Address)'와 같은 일반적인 라벨 대신에 '조지 워싱턴(George Washington)'이나 '1600 Pennsylvania Ave'와 같은 실제와 비슷한 가명을 사용한 경우, '검토자가 가명과 남은(누설된) 식별자를 구분할 수 없었기 때문에' 문서에 남아 있는 일부 성명의 재식별 위험이 낮아지거나 경감되는 것을 확인하였다.

이들 시스템들은 HIPAA 세이프 하버 정보 요소 18개를 제거하는 것 이외에는 비식별화를 시도하지 않아, 다른 정보를 이용하여 개인을 재식별할 가능성을 열어두었다. 예를 들면, 미국과 캐나다의 법규에 따르면 약물 부작용에 관해 보고해야 한다. 이러한 보고서는 기자와 연구자들이 사망 보고서와 뉴스 보도와 사망 등록 등의 다른 정보 출처를 연관시켜 재식별하였다.

7.2 사진과 비디오의 비식별화

정지 화상, 판매용 비디오, 감시용 비디오에는 개인을 식별하는데 사용할 수 있는 많은 정보가 있을 수 있다. 비식별화를 통해 비디오를 비식별화함으로써 특정한 용도로 사용하도록 하면서도, 이러한 식별정보를 삭제함으로써 개인이 식별되지 못하도록 한다.

사진이나 비디오를 찍었을 때 카메라가 생성하였거나 사후의 가공 도구를 이용하여 추가한 경우, 식별정보가 이미지 정보와 함께 이미지 파일에 내장된 메타정보 형태로 존재할 수 있다. 예를 들어, 어떤 사람의 주택의 GPS 주소, 카메라의 시리얼넘버, 또는 사람의 성명이 헤더에 내장되어 있을 수 있다. 이러한 개인정보를 비식별화하는 것과 관련된 이슈는 6장에서 다른 종류의 구조화된 정보를 비식별화하는 것에 관련된 이슈와 유사하다. 그러나 널리 알려지지 않은 바이너리 구조(binary structure)로 이러한 개인정보를 저장할 수 있기 때문에 더욱 문제가 복잡하다. 따라서 식별정보가 존재할 수 있지만, 알 수 없거나 감춰져 있을 수 있다.

또한 멀티미디어 컨텐츠 자체를 비식별화하려고 할 때 발생하는 다양한 이슈도 문제를 더욱 복잡하게 한다. 멀티미디어 컨텐츠에는 예를 들면 관찰자가 어떤 사람이 키가 크고 나이 든 여성임을 추론할 수 있도록 하는 등, 특정 인물을 식별할 수 있거나 개인의 신원에 제한을 가할 수 있는 정보가 많다.

ICT COST Action IC1206 "멀티미디어의 프라이버시 보호를 위한 비식별화"는 멀티미디어 컨텐츠에서 "얼굴, 목소리, 실루엣, 걸음걸이와 같은" 식별정보를 삭제하기 위한 방법을 모색하고 있다. 그러한 작업의 일환으로, 위원회는 멀티미디어 컨텐츠 안의 식별자 분류체계를 개발해왔다.

- 바이오인식인증 식별자, 개인을 식별하는데 사용하는 구분되고, 측정할 수 있으며, 일반적으로 특이성이 있고, 영구적인 개인적 특징. 생리학적 바이오인식인증 식별자(얼굴, 홍채, 귀, 지문)와 행동학적 바이오인식인증 식별자(음성, 걸음, 자세, 입술움직임, 타이핑 스타일) 등이 있다.
- 연성 바이오인식인증 식별자. 영구적이거나 구분되지는 않지만 모호한 신체적, 행동적이거나 사람에 부수된 특징(키, 몸무게, 눈 색깔, 실루엣, 연령, 성별, 인종, 사마귀, 문신, 점, 흉터)
- 비바이오인식인증 식별자. 문체, 어조, 특정 사회-정치적, 환경적 문안, 복장 스타일, 헤어스타일 등.

멀티미디어 컨텐츠의 비식별화에서는 이미지와 음향 정보(있는 경우)를 변경하여 식별을 어렵게 하거나 불가능하게 한다. 바이오인식인증, 연성 바이오인식인증, 비바이오인식인증 식별자는 함께 있는 경우가 많으며, 개인의 프라이버시를 보호하기 위해서는 이들을 모두 비식별화해야 한다. 이러한 작업을 다중모드 비식별화(multimodal de-identification)라고 할 수 있다.

초기 연구에서는 이미지를 변환하여, 자동 얼굴 인식 시스템을 이용하여 개인을 신뢰성 있게 식별할 수 없도록 하는데 목적을 두었다. 예를 들어, 사진 비식별화 기법을 대규모로 적용한 구글 스트리트 뷰(Google Street View)가 사용한 얼굴 흐리게 하기(face blurring)가 있다. 일부 연구자들은 몸을 식별하고 흐리게 할 수 있는 시스템을 개발하였는데, 이는 연구 결과에서는 얼굴이 없이도 몸을 식별할 수 있다는 점을 보여주었기 때문이다. 어떤 시험용 시스템은 특정 종류의 정지 이미지에서 식별문신의 위치를 확인하고 제거할 수 있는데, 품질이 낮은 정보, 복잡한 장면, 일부가 가려져 있거나 높은 곳에서 본 문신 또는 많은 원근이 포착되는 비디오에서 정지 이미지를 어떻게 처리하는지는 분명하지 않다.

사람의 이미지를 비식별화하는 것 이외에도, 음향과 문서에서 식별단서(identifying cue)도 처리해야 한다. Cunningham과 Truta는 개인정보를 최소한으로 손실하면서 발화자의 신원을 보호하는 말뭉치를 생산하는데 도움이 되는 '통제 음향 왜곡(controlled audio

distortion)'을 이용하였다. 물론 단순한 음향 왜곡을 통해서는 단지 발화자의 음성을 이용하여 식별을 방지할 수 있을 뿐, 발화 패턴이나 이름을 언급하는 등의 오디오 트랙에 있을 수 있는 다른 식별단서를 제거할 수 없다.

멀티미디어 비식별화의 효과 검증은 다음과 같은 문제가 수반된 다차원적인 문제이다.

- 비식별화가 필요한 대상의 식별 정밀도와 정확성 : 구글은 자사의 완전 자동 시스템이 얼굴의 89%, 번호판의 94~96%를 흐리게 할 수 있다고 보고하고 있다. 그럼에도 불구하고, 기자들은 많은 얼굴들이 흐리게 처리되지 않은 채로 있다고 구글을 비판해왔다. 기자들은 구글이 종교적 조상(彫像)의 얼굴을 흐리게 처리하였다고도 비판하였다. 어떤 경우에는 특정 사물, 상징, 또는 인물을 흐리게 처리하거나 달리 훼손하는 것이 용인되지 않을 수 있다.
- 변환의 가역성(reversibility) : 복수의 이미지를 조합하여 모자이크를 제거하고 흐린 이미지를 복원하는 기술이 있기 때문에, 모자이크처리(pixelation)나 흐리게 하기(blurring)를 이용하여 비디오를 모호하게 하는 경우에 주의해야 한다. 일부 연구자들은 모자이크처리나 흐리게 하기 대신에 얼굴을 합성된 얼굴 또는 완전히 다른 얼굴로 대체할 수 있는 시스템을 개발해왔다.
- 생성된 이미지의 시각적 품질 : 흐리게 하기와 모자이크처리는 이상한 그림을 만들어내어 장면에 대한 해석에 영향을 줄 수 있다는 단점이 있다.
- 선택한 신원 모호화 기법의 실제적인 효과 : 일부 연구자들은 얼굴 인식 소프트웨어에 비해 알고리즘에 높은 점수를 주지만, 복장, 자세, 공간-시간적 환경을 조합하여 사람을 식별할 수도 있다.

본 보고서의 앞 부분에서는 구조화된 개인정보와 문서의 비식별화의 효과를 정량화하기 위한 몇몇 시도를 논의하였지만, 멀티미디어 비식별화의 효과를 정량화 하기 위한 의미있는 노력은 확인된 바가 없다.

다양한 재식별 시나리오가 있기 때문에, 비식별화에 대한 적절한 검사는 복잡하다.

- 자동 식별화 시스템의 재식별 시도
- 훈련되어 있지만, 정보주체에 대한 개인적인 지식이 없는 사람에 의한 재식별
- 정보주체의 관련자나 친구에 의한 재식별.

7.3 의료 영상의 비식별화

과학적 연구 성과의 재현과 검증, 연구 정보 기반의 확대와 품질 평가 등 과학적, 운영적 목표를 달성하기 위해 보다 넓은 범위로 의료 영상을 공유하려는 욕구가 있다. 프라이버시에 대한 우려와 HIPAA 프라이버시 규칙에 따라, 이미지를 공유하기 전에 비식별화를 해야 한다. 의료 영상은 통상적으로 DICOM(Digital Imaging and Communication in Medicine) 양식으로 된 헤더 정보(메타정보)와 이미징 기기가 생성한 픽셀(pixel)(이미지

정보)로 이루어져 있다. 개인을 식별할 수 있는 정보는 헤더나 픽셀에 존재할 수 있다. 의료 이미지는 비식별화에 관한 다음과 같은 많은 문제를 야기한다.

- DICOM 헤더에는 환자의 성명 또는 기타 직접 식별자, 준-식별자가 포함되어 있을 수 있다.
- 픽셀에는 사진 정보 또는 개인을 분간할 수 있는 기타 바이오인식인증 정보가 있을 수 있다. 예를 들면, 병원이 사람 얼굴이 들어간 부상 사진을 찍을 수 있고, 여기에서 사람을 식별할 수 있다.
- 픽셀에 있는 정보를 수학적으로 처리하여 인식 가능한 이미지나 바이오인식인증 정보를 생산할 수 있다.
- 직접 식별자가 인간이 읽을 수 있는 문서 형태로 픽셀 안에 내장되어 있을 수 있다. 예를 들면, 이미지를 만들 때 디지털화하거나 사진으로 포착한 개인기록부에 수기로 환자의 성명을 써놓을 수 있다. 그 대신에 소프트웨어를 이용하여 이미지 안의 예측 가능 하거나 지정된 위치에 문서를 스캔(burn-in)할 수 있다.

다른 파일 양식과는 다르게, DICOM 표준에는 헤더나 이미지의 픽셀 구역에 식별정보가 존재하는지를 지정하고, 어떤 파일이 비식별화되었는지 지정하기 위한 조항이 있다. 예를 들어, DICOM의 픽셀정보 삭제 옵션(Clean Pixel Data Option)을 지정하면, 식별정보가 픽셀 정보로 스캔되었는지 표시할 수 있다. 만약 인식 가능한 시각적 특징 삭제 옵션(Clean Recognizable Visual Features Option)을 지정하면, 픽셀 정보 안의 정보를 이용하여 개인을 인식할 수 있는지를 표시할 수 있다. DICOM PS3.15 부속서 E, 속성 비밀 프로파일(Attribute Confidentiality Profiles)에는 비식별화된 DICOM 이미지를 생산하기 위한 구조화된 절차가 명시되어 있다. 즉, 식별정보를 암호화하여 '암호화 속성 정보 집합(Encrypted Attributes Dataset)'에 저장함으로써 비식별화된 파일을 나중에 재식별할 수 있다.

그러나 DICOM 표준은 비식별화를 위한 실제 알고리즘이나 기법을 명시하고 있지 않다. 그러한 기법은 각각의 이미지 작성 방식에 따라 다를 것이며, 다음과 같이 활발하게 연구가 진행되고 있는 분야이다.

- Freymann 등은 이미지를 공개 아카이브에 저장하기 전에 DICOM 헤더 정보를 비식별화하기 위한 오픈 소스 소프트웨어 세트를 개발하였다. 저자들은 상용 소프트웨어는 DICOM 스캔 표시기가 지원되지 않기 때문에, 스캔 방지 의료 정보를 스캔하는 도구가 필요하다는 점에 주목하고 있다.
- 몇몇 연구자들은 컴퓨터 단층촬영(CT) 및 자기공명(MR) 영상으로 만든 3차원 모델을 이용하여 사람의 얼굴을 수학적으로 재구성하기 위한 기법을 시연해왔다. 연구자들은 이러한 위협에 대응하기 위해 얼굴을 만드는데 사용할 수 있지만 진단용으로는 활용 가치가 없는 MRI 이미지 부분을 자동으로 제거하기 위한 기법을 개발해왔다.

7.4 유전 정보와 생물학 자료의 비식별화

유전자 서열과 기타 서열 정보는 HIPAA 프라이버시 규칙에서 개인을 식별하는 정보로 간주되지 않는다. 일부 유전자 서열은 매우 개인적이고, 현재 명시적으로 개인을 식별하기 위하여 유전자 정보를 일상적으로 수집하여 데이터뱅크에 넣기 때문에, 일부 평론가들은 프라이버시 규칙에 관련 내용이 없다는 점을 비판해왔다.
더욱이, 유전자 정보는 유전되기 때문에, 자신은 유전자 서열이 확인되지 않았지만, 대신에 친척의 유전자 서열이 식별 데이터베이스에 포함된 사람의 신원을 확인하는데 유전자 서열을 이용해왔다.

다음과 같은 사례가 있다.

- 2005년에 나이가 15세인 한 소년이 DNA 테스팅 서비스 업체인 FamilyTreeDNA.com을 이용하여 정자를 제공한 아버지를 찾았다. 비용이 289달러인 이 서비스는 이 소년의 아버지를 식별하지 못했지만, Y염색체가 일치하는 남자 2명을 식별하였다. 두 남자의 성(姓)은 같았지만 철자가 달랐다. Y 염색체는 아버지에게서 아들로 그대로 전해지기 때문에 유럽의 성(姓)과 같은 방식으로 유전되는 경향이 있다. 정자 제공 일자와 출생지(이 정보는 소년의 어머니에게 제공되었다)와 이 정보를 이용하여 이 소년은 현재 '유전관계 삼각측량(genealogical triangulation)'이라고 알려진 온라인 검색 서비스를 이용하여 아버지를 식별할 수 있었다.
- 2013년에 MIT 연구 팀은 이 실험을 연장하여, 인간 다형성 연구(the Study of Human Polymorphisms, CEPH)와 1000 게놈 프로젝트(1000 Genomes Project)의 일부로 DNA 검사 결과가 인터넷에 공개된 50명 이상의 성(姓)과 완벽한 신원을 식별하였다.

Erlich와 Narayanan은 유전자 서열을 재식별하는 기법과 그러한 공격을 방어할 수 있는 기술적 조치에 관한 자세한 검토결과를 공개하였다. 현재로서는 재식별에 필요한 최소한의 유전자 서열 크기에 관한 과학적 합의는 없다.
또한 재식별을 금지할 데이터 이용 합의서를 집행할 필요 없이 연구자들이 비식별화된 유전자 정보를 이용하도록 하기 위한 적절한 메커니즘에 대한 합의도 없다.

7.5 지리 정보와 지도 정보의 비식별화

지리 정보의 비식별화는 연구가 활발한 분야이다. 현재의 방법은 인자변환(perturbation)과 일반화(generalization)에 의존하고 있다. 인자변환은 일부 경우에 문제가 있을 수 있다. 왜냐하면 예를 들면 식당이 물속으로 움직인다든지, 인자변환된 위치가 상식에서 벗어날 수 있기 때문이다.
그러나 특히 집단의 분포가 분산되어 있거나 복수의 관찰 결과를 연관시킬 수 있는 경우에는(특히 관찰 결과가 다른 일반화 영역을 이용하는 경우), 일반화로는 신원을 감추기에 불충분할 수 있다. 일종의 일반화나 인자변환이 없다면, 위치를 비식별화하기가 매우 어

려울 수 있는 지리적 정보가 매우 다양하다. 예를 들면, 일정한 기간에 걸쳐 측정한 핸드폰의 가속도계를 이용하여 움직임을 거리 그리드(street grid)에 끼워 넣어 위치를 추론할 수 있다. 따라서 일정 기간에 걸쳐 샘플링한 가속 운동은 공개된 정보와 조합할 경우에 식별정보가 될 수 있다.

부 록 Ⅰ-1

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

지식재산권 확약서 정보

해당사항 없음

Ⅰ-1.1 지식재산권 확약서(1) (스타일 적용-대항목/소항목)

- 발명의 명칭
- 권리자의 성명
- 등록(출원) 번호
- 등록(출원) 연월일
- 실시조건
- 확약서 접수일

Ⅰ-1.2 지식재산권 확약서(2) (스타일 적용-대항목/소항목)

- 발명의 명칭
- 권리자의 성명
- 등록(출원) 번호
- 등록(출원) 연월일
- 실시조건
- 확약서 접수일

※ 상기 기재된 지식재산권 확약서 이외에도 본 기술보고서가 발간된 후 접수된 확약서가 있을 수 있으니, TTA 웹사이트에서 확인하시기 바랍니다.

부 록 Ⅰ-2

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

시험인증 관련 사항

해당사항 없음

부 록 Ⅰ-3

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

본 기술보고서의 연계(family) 표준

해당사항 없음

부 록 Ⅰ-4

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

참고 문헌

[1] ISO 25237 Health informatics - Pseudonymization, http://www.iso.org

부 록 Ⅰ-5

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

영문기술보고서 해설서

해당 사항 없음

부 록 Ⅰ-6

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

기술보고서의 이력

판수	채택일	기술보고서번호	내용	담당 위원회
제1판	2018.09.	제정 TTAx.xx-xx.xxxx	개인의료정보의 비식별화	PG505